hack·er (hăk'ər)

"Persona che si diverte ad esplorare i dettagli dei sistemi di programmazione e come espandere le loro capacità, a differenza di molti utenti, che preferiscono imparare solamente il minimo necessario."

Un pò di **pace**

"Amo il lavoro; mi affascina. Posso star seduto a guardarlo. Adoro tenermelo vicino; l'idea di liberarmene mi spezza il cuore."
Jerome K. Jerome

Questo giro non vorrei fare polemiche, so che molti di voi resteranno stupiti e forse delusi, fa caldo e chiudere questo numero di HJ ci ha divertito e dato un gusto che alle volte un po' viene a mancare. Abbiamo un sacco di cose in questa uscita, abbiamo un po' di "hardware ecologico", il concetto di eco compatibilità e impatto ambientale è importante per noi e per chiunque voglia vivere su questo pianeta non da tiranno ma da creatura appartenente ad un sistema. Abbiamo una sfida che vi lanciamo con strumenti antichi come l'uomo, gli indovinelli e la criptografia, abbiamo un paio di articoli dedicati al pinguino con cui sicuramente vi divertirete. Abbiamo tutto sul nuovo Firefox e un paio di pagine per gli amanti della Mela. Insomma, ci sembra un bel numero e noi ci siamo divertiti a farlo, spero che sarà altrettanto divertente per voi leggerlo.

Un ultima cosa, abbiamo inaugurato un piccolo blog (www.bigg-theguilty.blogspot.com) dove posteremo i nostri editoriali e magari materiale inerente la rivista ma che magari, per motivi di spazio, non riusciamo a pubblicare e intanto stiamo riprendendo in mano la questione del sito... Con la calma e la pazienza sistemeremo tutto, abbiate fede.

The Guilty

CONTINUA LA CACCIA

In tanti ci hanno già risposto ma non ci basta mai e vogliamo solo il meglio per le nostre pagine e i nostri lettori e quindi continuate a mandare le vostre candidature alla mail:

contributors@hackerjournal.it

HACKER JOURNAL: INTASATE LE NOSTRE CASELLE

Diteci cosa ne pensate di HJ, siamo tutti raggiungibili via e-mail, tramite lettera o messo a cavallo... Vogliamo sapere se siete contenti, critici, incazzati o qualunque altra cosa! Appena possiamo rispondiamo a tutti, scrivete!

redazione@hackerjournal.it

Anno 8 – N.155
10/23 luglio 2008

Editore (sede legale):
WLF Publishing S.r.l.
via Donatello 71
00196 Roma
Fax 063214606

Printing:
Roto 2000

Distributore:
M-DIS Distributore SPA
via Cazzaniga 2 - 20132 Milano

Copertina: Daniele Festa

HACKER JOURNAL
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.

Una copia 2,00 euro

Direttore Responsabile:
Teresa Carsaniga

Sempre più PC, sempre più PERICOLI

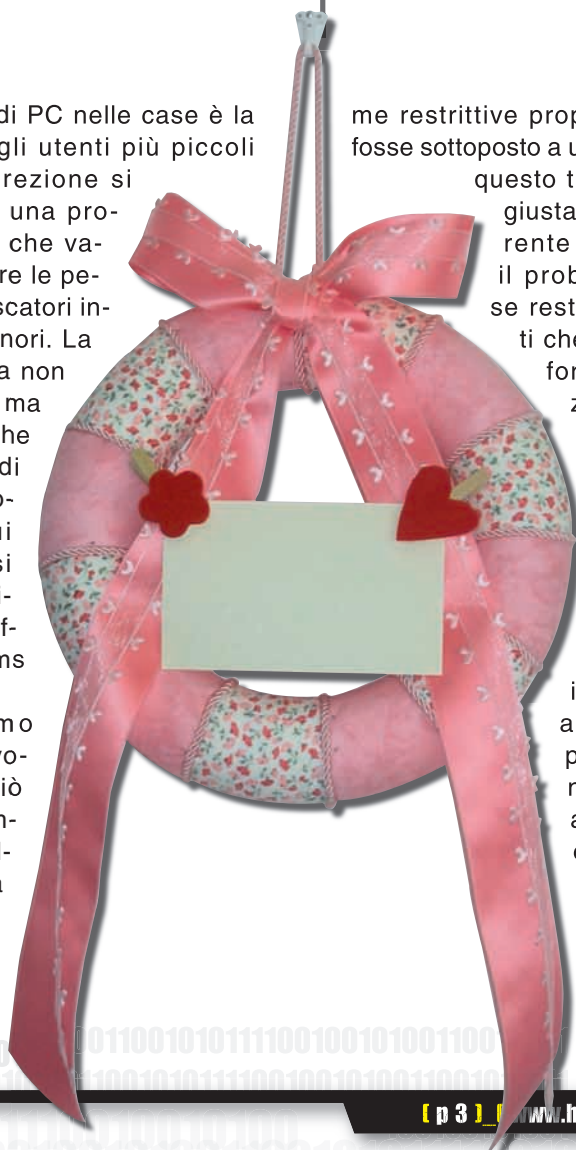
Aumenta ancora il numero di computer venduti al mondo e, assieme a questo, devono aumentare le tutele per chi questi computer li usa

Arriva dall'istituto di ricerca statunitense Gartner una nuova ricerca sulla diffusione dell'uso del computer al mondo secondo la quale attualmente sarebbero 1.000.000.000 di computer al mondo. La maggior parte, il 58% è stato acquistato tra USA e Europa ma si prevede che entro sei anni i computer saranno 2.000.000.000 e del nuovo miliardo che arriverà il 70% sarà acquistato tra Brasile, Cina e India, tutti paesi in fortissimo sviluppo.

L'incremento massiccio di vendite è da imputare ai prezzi sempre più accessibili delle macchine e dalla percezione comune che sia ormai impossibile vivere senza computer, cosa che possiamo anche ritenere vera ;-)

Uno dei problemi maggiori dati da questa ondata di vendite è invece l'aumento vertiginoso della spazzatura elettronica che, come ben sappiamo, non è di facile smaltimento.

Il secondo, non per importanza, problema dato dalla sempre più capillare presenza di PC nelle case è la protezione degli utenti più piccoli e in questa direzione si sta muovendo una proposta di legge che vada ad aumentare le pene per gli "adescatori informatici" di minori. La legge si occupa non solo di Internet ma comprende anche le altre forme di grooming, il processo con cui l'adescatore si insinua nella vita del minore, effettuate con sms o mms.

Non possiamo che essere favorevoli a tutto ciò che vada a combattere una delle piaghe della nostra rete come la pedofilia, l'inasprimento delle pene e le forme restrittive proposte per chi fosse sottoposto a un processo di questo tipo sono una giusta forma deterrente per limitare il problema anche se restiamo convinti che l'unica vera forma di protezione verso i minori sia la presenza di adulti responsabili nella loro vita, anche informatica, che possano insegnare loro a distinguere le persone, anche virtuali, con cui si interfacciano e che possano fornire una guida anche nel surfing sulla rete. ■

YouTube SUL MINICINEMA

YouTube introduce una nuova sezione nel suo sito. Ora gli utenti avranno la possibilità di scaricare a pagamento produzioni cinematografiche indipendenti e di offrire quindi, contenuti di più ampio respiro su DVD come in download digitali.
Il nuovo servizio è chiamato Screening Room, vi è la possibilità per i filmmaker di inserire video sui server di Google dalla lunghezza massima di 1 Gigabyte. Una dimensione sufficiente, ad esempio, per stipare un film in definizione standard su iTunes, e quindi adeguata alle nuove possibilità di distribuzione offerte dal portale.

CYBER-DIFESA EUROPEA

La NATO ha deciso che sorgerà in Estonia il primo e prossimo centro di addestramento per la cyber- difesa europea. Parte, quindi, da questo paese, che solo l'anno scorso si è visto in serio pericolo per l'attacco massicio sulla propria rete nazionale, il grane progetto per una difesa informatica a prova dei migliori criminali informatici. I paesi che hanno costituito questo ordine sono: Estonia, Italia, Germania, Lituania, Slovenia, Lettonia e Spagna.

Il centro di difesa aprirà però solo il prissimo anno mentre i 30 esperti informatici che ne fanno parte saranno operativi e inizieranno a lavorare già dal prossimo agosto. Rimane solo qualche dubbio sulle basi economiche, visto che le nazioni europee interessate sembra abbiano le braccine un po' corte, che potrebbero essere risolto da cooperazioni internazionali. A farne parte potrebbe essere proprio una piattaforma di consulenza di alto livello come la neo IMPACT, che nota nomi di alto livello come il CEO di Symantec John Thompson e un vero condor della rete come Vint Cerf.

U.S.A. A RISCHIO

La Government Accountability Office ha dichiarato, con una seria preoccupazione sulla vulnerabilità della più grande rete energetica del paese americano. La Tennessee Valley Authority (TVA) avrebbe una grossa falla di sistema che permetterebbe un rischioso sabotaggio mettendo ben 8,7 milioni di persone in serio pericolo. la TAV, che gestisce in America 11 impianti a carbone, 8 turbine a gas, 3

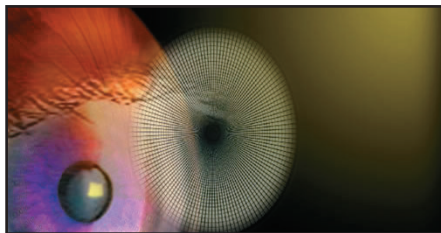
impianti nucleari e 29 centrali idroelettriche, non supera gli standard di sicurezza previsti per le infrastrutture federali mancando di aggiornamenti adeguati su antivirus, protezioni specifiche su firewall, e di sistemi di monitoraggio del network. Nulla di più allettante per creare un 11 settembre informatico insomma.

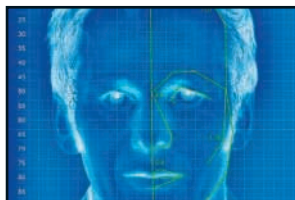
WINDOWS FA A CAZZOTTI CON SAFARI

Proprio in questi giorni arriva un nuovo attacco da parte di Microsoft ai danni di Apple. Infatti in una conferenza stampa, Microsoft, afferma che ci sono ancora troppi problemi di vulnerabilità nel momento in cui si installa Safari sui sistemi operativi Windows, sia che siano Vista sia che siano XP.
Il rischio è di ritrovarsi il PC infestato da

HOT NEWS

TOSHIBA FREGATA DAI GEMELLI

Tutti noi sognamo un mondo informatico più efficace ed evoluto. Sempre meno legato dai codici e dalle password che poi alla fine non ti proteggono neanche come dovrebbero. Ed è per tutti noi che Toshiba ha messo in produzione e in-vendita il nuovissimo software Face Recognition, che si può trovare già nei neo-laptop Toshiba Satellite A305-S6845. Face Recognition non è altro che un sistema di riconoscimento facciale, legato alla scansione del proprio volto mediante microcamera. La quale invia poi i dati alla codificazione e quindi al riconoscimento. È molto più facile da usare che da impostare data la lunga procedura di riconoscimento iniziale ma una volta eseguita la prima cosa da provare è accedere al proprio account PC senza dover digitare la solita password. Un particolare, invece, alla quale Toshiba sta già ponendo rimedio è la netta vulnerabilità sul sistema di riconoscimento quando i soggetti umani sono gemelli.

10 FALLE PER ME...

Microsoft ha reso pubblico un report contenente informazioni riguardanti 10 vulnerabilità dei sistemi operativi Windows. Le falle del sistema oprativo riguardano i programmi Office, Internet Explorer e DirectX. I buchi dannosi sono stati rilevati nello svolgimento di aoperazioni sul Bluetooth di Windows XP e Vista (MS08-030), ad Internet Explorer 5, 6 e 7, (MS08-031) e alla tecnologia DirectX 7, 8, 9 e 10 Altri tre bollettini sono classificati come "importanti", e riguardano vulnerabilità nel Windows Internet Name Service (WINS) di Windows 2000 Server e Windows Server 2003 (MS08-034), nel componente Active Directory di Windows 2000 Server, Windows XP Professional, Windows Server 2003 e Windows Server 2008 (MS08-035), e nel protocollo PGM (Pragmatic General Multicast) implementato in tutte le versioni ancora supportate di Windows, dalla XP alla 2008 (MS08-036). Insomma un bell'elenco di porte aperte... sempre che ci sia qualcuno capace di entrare.

ARRIVA OPERA 9.5

In questi giorni è uscito Opera 9.5, ultima versione dlla casa Opera Software. Dalla versione 9.2 il nuovo Opera ha migliorato tantissimo la compatibilità con i siti internet e lo scambio di dati con le interfaccie grafiche di Mac e Linux. La casa costrutricce dichiara, inoltre, che la nuova versione è due volte più veloce della precedente. Una delle caretteristiche più interessanti è la funzionalità di Quick Find che è in grado di ritrovare in poco tempo pagine web già visitate archiviandole nel proprio sistema operativo con i collegamenti a testi ed immagini in maniera temporanea. Il nuovo Opera fornisce anche la possibilità di sincronizzare, via Internet, gli indirizzi dei segnalibri e quelli associati alla funzione Speed Dial: la sincronizzazione funziona sia tra due PC, sia tra un PC e un telefono cellulare dotato di Opera Mini. Opera Software considera questa realease una versione completa di tutto.

malware senza avere la possibilità di controllare l'accesso o avere la possibiità di eliminarli definitivamente.
Microsoft accusa Safari di non saper ancora gestire in maniera esaudiente la modalità di scaricamento di molti file che entrano nel nostro computer senza essere rilevati dagli antivirus o dalle protezioni di sistema. Noi personalmente non ci siamo stupiti di tali affermazioni essendo Safari un software di Apple una marca che non sviluppa molto nel campo della sicurezza avendo un sistema operativo poco interessante agli occhi dei pirati informatici e dei siti spazzatura.

Il malware ti fa diventare pedofilo

Ha fatto male, Michael Fiola di Boston, negli Stati Uniti, a lasciare per così tanto tempo il proprio laptop vulnerabile agli attacchi di malware di diverso tipo, worm e trojan. Infatti, sul suo portatile sono state scaricate immagini di pornografia infantile. Micheal è stato accusato di pedoporno grafia dallla polizia di Boston che però ha ritirato le accuse al 53enne americano perché non ha scaricato di propria volontà quelle foto, probabilmente non le ha proprio mai viste, ma lo ha fatto il malware che aveva infettato il suo PC. Una decisione che lo assolve, dunque, da un'accusa infamante, quella di contribuire alla diffusione di immagini realizzate abusando di bambini, ma una decisione che arriva tardi, che non consentirà a Fiola di riavere la vita perduta per un trojan di troppo.

IL PROFESSOR MILNER

Il professor Robin Milner è stato premiato con il premio Turing, la massima onorificenza per chi lavora nel capo della ricerca informatica.
Tra le più famose teorie del professore ci sono il pi-calcolo, lo studio dell'inferenza di tipo e l'analisi dei sistemi concorrenti. Al suo discorso ha detto: "Ai tempi di Alan Turing l'informatica e la scienza della computazione erano una sorta di foglio bianco, sul quale Turing stesso ha lasciato una traccia. Oggi le cose sono diverse, c'è molta più specializzazione degli studiosi nei diversi campi: ma siamo davanti ad una nuova età dell'oro, nella quale ci sono molti fogli bianchi da riempire con le scoperte di molti altri ricercatori". Noi della redazione facciamo i più sentiti complimenti al professor Milner.

L'ITALIA È IN EUROPA?

In questi giorni si parla tanto di sicurezza informatica in Europa e in particolar modo in Italia. Per quello che ci fanno capire intendono sicurezza informatica un sinonimo di tracciare l'utenza internet. Ci sono e verranno vagliate procedure che permettono e garantiscono, secondo loro, una tracciata di tutto quello che può fare o visitare un utente sul web. A questi rigori però non sono stati i proprietari di un noto locle di Trieste che si sono visti multare di 1.036,00 € per non aver preso nota e registrato gli utenti che utilizzavano internet tramite la rete wireless gratuita messa a disposizione dal ristoratore. Non vogliamo dire che sia giusto o sbagliato tutto ciò ma solo che a nostro parere ci sembra abbastanza contradditorio. Contradditorio perché da una parte abbiamo l'esempio di molte città e capitali europee dove è possibile collegarsi a internet gratuitamente anche in strada e dall'altro lato un esempio simile che però in Italia viene multato per non aver preso nota di documenti personali del tutto contraffabili.

38 PHISHERS ARRESTATI

38 pirati informatici, a noi piace chamarli così e non Hackers come li definisce la Cyber-Cop dell'F.B.I., sono stati finalmente acciuffati con le mani nel sacco dopo aver saccheggiato molti conti correnti, operazione resa possibile da una seria scrematura di possibili vittime milionarie alle quali sono state rubate informazioni personali bancarie e clonazioni di carte di credito.
La maggior parte dele informazioni sulle vittime veniva presa da un centro di dislocamento in Romania per poi essere inviate in Virginia dove venivano scremate sulla base della maggior disbonibilità di trasferimento contante possibile in un solo prelevamento. I noti phishers lavoravano in gruppi di persone appartenenti a diversi stati come: Romania, Virginia, Vietnam, cambogia, Pakistan e Messico. I malfattori sono stati tutti accusati di furto di identità, clonazione di carte di credito, produzione e traffico in dispositivi di accesso contraffatti, frode bancaria, accesso non autorizzato a computer protetti; quanto basta per assicurarsi una lunga vacanza in prigione.

SALVIAMO MAMMA JAMMIE

Jammie Thomas è stata condannata al risarcimento di 200mila dollari per il violamento delle norme di copyright e i diritti di distribuzione dei contenuti negli States. Sono stati, però, 10 professori a fare da controparte, proteggendo Jammie affarmando che limitarsi a rendere disponibile un'opera al pubblico, sia su Internet o in qualsiasi altro modo, di per sé non costituisce una distribuzione. Questo ha spiazzato tanto la Copyright Act, parte accusante, quanto i giudici che hanno fermato l'inchiesta per riunirsi alla luce delle nuove informazioni fornitogli.
Ora Jammie Thomas è inattesa di sapere l'esito della sua condanna ma rispetto all'inizio ha dieci angeli che la sostengono.

UN'ALTRO PASSO VERSO TERMINATOR

È il promettente parto di un team di ricercatori della Facoltà di Informatica della Universidad del Pais Vasco, si ispira alla mitologia basca fin dal suo nome, Tartalo, ed è un robot. L'idea di fondo dei ricercatori che ci stanno lavorando sopra è di costruire un apparato informatico che consenta al robot di girovagare da solo. L'obiettivo finale è far

VERSO LA VERA TECNOLOGIA

È stato presentato a il mese scorso in Slovenia e in questi giorni a Verona, il progetto per la sicurezza informatica **AVANTSSAR.** Si tratta di un progetto che prevede l'impiego di 50 ricercatori, 10 partner europei e 6 milioni di euro di budget; che serviranno a proteggiere maggiormente lo sviluppo di nuove tecnologie generazionali che usciranno dai laboratori informatici. Questo ambizioso progetto non tratta solo l'elemento informatico ma anche e-health, mezzi di trasporto e di commercio. Tutti sevizi che sono stati ultimi protagonisti del rapido cambiamento delle infrastrutture della società, come dice il docente universitario veronese Viganò. In oltre fa sapere che il principale obbiettivo, di questo progetto, è quello di garantire in forma sicura, veloce ed automatica la sicurezza dei servizi che potrebbero esserci ma non ci sono ancora per i troppi problemi di sicurezza. Un modo per farci capire che con maggiore sicurezza un giorno si potrebbe avere l'effettivo vantaggio da una tecnologia che ormai ci ha superati ed ora è li che ci aspetta.

MAPPATURA DEL MAL WEB

"Hong Kong e Cina sono le patrie dei siti più malevoli del nostro pianeta". A dirlo è la McAfee che ha preso in esame 10 miolioni di siti facenti capo a 265 estensioni diverse. Insomma sarebbero i siti .hk e .cn, con i rispettivi 19% e 12% di paricolosità ad infettare i nostri PC. È stato pubblicato dalla McAfee la seconda edizione di "Mappatura del Mal Web", un simpatico ed utile rapporto dove vengono spiegati i criteri di esaminazioni di tutti questi siti e nella quale possiamo trovare un dettagliato elenco, con i risulati in percentuale di rischio.
Al terzo posto di questa classifica troviamo i siti .info con l'11% , a seguire vengono i siti . ro, Romania con il 6,8%, e .ru, Russia con il 6%. Non molto lontano troviamo il consueto .com con il 5%.
i migliori classificati, secondo questo elenco, sarebbero i .au australiani con lo 0,3 i .jp del Giappone con lo 0,1% e quelli .gov, siti governativi con il 0,05%.
Ricordiamo però che chiunque i qualsiasi parte del mondo può registrare domini quindi non dobbiamo legare volutamente le estensione di questi siti con la "faccia" del paese che li rappresenta.

2,5 POLLICI X 500 GB

Samsung ha introdotto nel mercato globale il suo primo hard disk da 2,5 pollici da 500 GB.
Lo Spinpoint M6, ha una velocità di rotazione di 5400 RPM, 8 MB di cache, un'interfaccia SATA da 3 Gbps e un sensore di cadute opzionale.
A differenza dei suoi imminenti rivali, il TravelStar 5K500 (5400 RPM) di Hitachi e l'MHZ2 BT 500GB (4200 RPM) di Fujitsu, che condividono uno spessore "fuori standard" di 12,5 millimetri, l'hard disk di Samsung conserva lo spessore tipico, pari a 9,5 mm, dei tradizionali hard disk mobili: ciò lo rende compatibile con la quasi totalità dei notebook SATA oggi sul mercato.

sì che possa muoversi da un punto ad un altro di una città come farebbe un umano.
Il team leader Basilio Sierra garantisce che il roboot è in grado di riconoscere gli oggetti, l'ambiente circostante e di muoversi in piena indipendenza. Un'altro passo verso Terminator?!

ERRATA CORRIGE

Sul numero 153 di Hacker Journal, l'articolo di Francesco Principe "Essere Hacker Oggi", per un disguido, erano presenti alcuni errori di cui ci scusiamo con i lettori e con gli intervistati, i Chocolate Makers di cui mancava il riferimento internet: http://security.dico.unimi.it.

:: INTERVISTA

Essere Hacker Oggi

Molto tempo è passato dai primi voli del Condor è gli hacker sono cambiati, scopriamo come con un intervista alla crew italiana che ha vinto il Capture the Flag

Una volta definirsi Hacker aveva un gusto particolare. Gli Hacker erano figli di una corrente di pensiero nuova, primigeni della tecnologia e antagonisti naturali di quelle regole che volevano il mondo digitale imbrigliato e guidato da un'autorità centrale massificante, fredda, calcolatrice. Generalmente non erano affatto "cattivi" come sono stati dipinti dalla stampa e solo raramente sono stati dei fuorilegge. Negli anni in cui ebbero la massima visibilità, il Condor imperversava indisturbato per i server governativi americani e non era ancora stato catturato dalla FBI. Avevano costruito il proprio immaginario su film come Wargames e sui romanzi di Gibson.

And the winne is: CHOCOLATE MAKERS
Special mention for WCSC who hacked the challenge server

EVOLUZIONE della specie

Ancora più veloce e versatile, ecco il resoconto del primo test sul nuovo Firefox e di una chiacchierata con uno dei boss della volpe che ci spiega perché ora è più sicura

Il duello tra Internet Explorer e Firefox prosegue serrato. Mentre Microsoft prepara la versione 8 del suo browser, disponibile per ora in una versione beta destinata agli sviluppatori, il concorrente Mozilla vara la terza versione del fenomenale Firefox, puntando addirittura al Guinness dei primati.

:: Idea vincente

Lo sviluppo della terza versione di Firefox ha richiesto tre anni di lavoro ed è stata affidata a un gruppo di 150 programmatori sparsi in mezzo mondo. Mai come in questo caso, la filosofia Open Source ha mostrato tutte le sue potenzialità: le versioni Beta e Release Candidate sono state installate e provate da migliaia di persone, che hanno così contribuito a individuare e correggere gli errori nel programma e migliorarne le funzioni.
Il rilascio della versione definitiva, avvenuto proprio mentre mandiamo in stampa questo numero di Computer Magazine, è dunque il frutto di un impressionante lavoro collettivo, che ha coinvolto migliaia di persone in ogni parte del Pianeta. Nessuna rivoluzione, ma tanti piccoli miglioramenti e modifiche che rendono il programma ancora più versatile e comodo da usare.

Ai concorrenti non rimane che accettare la superiorità del celebre browser Open Source e studiarne le caratteristiche per cercare di seguirne le orme.

:: Colpo d'occhio

Il sistema di controllo ha subito variazioni minime: icone più elaborate e accattivanti, in particolare è rimasta identica la struttura a schede, molto apprezzata dagli utilizzatori, e la possibilità di modificare la barra degli strumenti trascinando pulsanti e controlli attraverso la funzione Personalizza.
Per quanto riguarda le modifiche "sotto il cofano", invece, gli sviluppatori hanno annunciato per la nuova versione oltre 15.000 tra aggiornamenti e modifiche rispetto all'edizione precedente. Al di là dei numeri, Firefox 3 può contare su un nuovo sistema di gestione Java e migliori prestazioni con Flash e vari contenuti attivi, come quelli per il controllo degli acocunt su Gmail. È bene ricordare, però, che il guadagno in termini di tempo necessario per la visualizzazione delle pagine, si calcola nell'ordine dei millisecondi.

Quando digitiamo un nome nella barra degli indirizzi, Firefox analizza i Segnalibri e la Cronologia per visualizzare tutti i siti che hanno attinenza con quello che stiamo scrivendo.

:: Ricerca intelligente

Una delle maggiori novità riguarda la barra degli indirizzi.
La versione 3 di Firefox, infatti, sfrutta un sistema che analizza in tempo reale le parole che digitiamo nella barra degli indirizzi e visualizza una serie di suggerimenti basati sulla corrispondenza con i Segnalibri e i siti Internet che abbiamo visitato recentemente.
Si tratta di uno strumento efficace, che rende la nostra navigazione molto più rapida e "naturale", ma che segna un'inversione di rotta nello sviluppo del browser. Le precedenti versioni di

Firefox, infatti, si distinguevano per la grande attenzione rivolta alla sicurezza e alla protezione dei nostri dati riservati, tutelati dalla funzione che consentiva di eliminare la cronologia dei siti visitati a ogni chiusura del browser. Ora l'uso di questa funzione ci impedirebbe di sfruttare una delle più interessanti novità del programma.
Un discorso simile vale per la nuova funzione che ci consente di salvare su disco il contenuto delle schede al momento della chiusura di Firefox, consentendoci di visualizzarle immediatamente nella nuova sessione di navigazione.

Per quanto possa risultare comodo, questo strumento può infatti trasformarsi in un vero "attentato" alla privacy, consentendo a chiunque metta le mani sul nostro PC di vedere quali siti abbiamo visitato nel corso dell'ultimo utilizzo del browser.

GUINNES DEI PRIMATI

In occasione del rilascio di Firefox 3, la comunità Open Source ha intenzione di entrare nel mitico Guinness dei primati stabilendo il nuovo record di download in 24 ore. L'obiettivo è stato centrato totalizzando oltre 8.000.000 download nel corso del 17 giugno. Al di là dell'aspetto più "frivolo", il record rappresenta un'impressionante dimostrazione di forza nei confronti dei produttori concorrenti. Firefox, infatti, conferma di essere il browser più apprezzato dagli appassionati del Web.

Firefox 3 integra un sistema di certificazione dei siti Internet che permette di verificarne l'autenticità. Uno strumento davvero efficace per arginare il fenomeno del phishing.

:: L'indice dei segnalibri

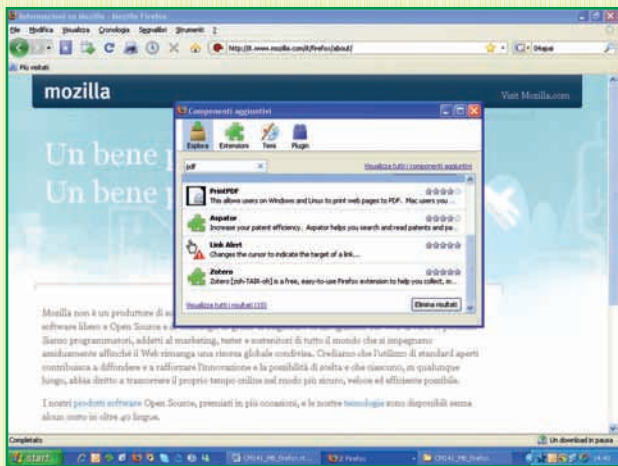
Il sistema di analisi delle parole digitate non si basa solo sulla corrispondenza con gli indirizzi memorizzati dal browser. Molti siti Internet, infatti, hanno indirizzi o nomi estremamente complicati, che potremmo scordare facilmente. Ora possiamo superare questa difficoltà grazie a un efficace sistema di Tag. In pratica, possiamo assegnare a ogni segnalibro una serie di parole chiave. Quando digitiamo una di queste, il programma propone automaticamente un elenco dei siti collegati, permettendoci di risparmiare qualche clic ed evitare di scorrere tutte le voci alla ricerca del sito che ci interessa.
Qualche cambiamento anche per la gestione delle password. Al posto della vecchia finestra pop up, ora i controlli per decidere se memorizzare o meno la password per l'accesso ai servizi Internet compaiono in una barra degli strumenti che dunque non disturba la navigazione.

:: Estensioni e Plugin

Uno dei punti di forza di Firefox è, da sempre, la possibilità di potenziare il programma installando le tante estensioni realizzate da programmatori indipendenti. La nuova versione mette a nostra disposizione un sistema più efficace per la ricerca e l'installazione: mentre prima dovevamo cercare le estensioni sul sito di Firefox, ora il tutto avviene attraverso la sezione Esplora della finestra Componenti aggiuntivi. Il sistema di ricerca è basato su parola chiave ed è presente anche un elenco di estensioni "consigliate" in base alla loro popolarità.
Nella stessa finestra troviamo anche una nuova sezione, chiamata Plugin. Da qui possiamo visualizzare una lista completa degli elementi aggiuntivi che risultano installati. Si tratta in molti casi di moduli indispensabili per navigare, come quello che garantisce il supporto per Flash o Java. Controllando l'elenco, però, ci rendiamo conto che molti software installati sul nostro computer installano automaticamente dei moduli di cui ignoravamo l'esistenza.

:: Professionista del download

L'uso delle estensioni non rappresenta solo uno dei punti di forza di Firefox. Per gli sviluppatori, il sistema delle estensioni ha rappresentato un ottimo osservatorio per individuare quali siano le esigenze degli utilizzatori. Con la nuova edizione del browser, i programmatori della comunità legata a Firefox hanno quindi deciso di integrare

La memorizzazione delle password non avviene più attraverso la finestra di pop up, ma tramite una barra aggiuntiva che non disturba la visualizzazione del sito.

Il nuovo sistema di gestione delle estensioni non richiede più il collegamento al sito. Tutto avviene all'interno della finestra Componenti aggiuntivi.

nel programma le funzioni più apprezzate degli utilizzatori, "clonando" le estensioni più popolari e rendendole parte integrante del browser.
Tra queste una migliore gestione dei download, che ora possono essere interrotti e ripresi anche se chiudiamo Firefox o riavviamo il computer. Il sistema di controllo è stato modificato solo lievemente, allo scopo di offrire una maggiore visibilità e leggibilità delle informazioni.

:: Sicurezza assoluta

Quando si parla di browser, il profilo della sicurezza è uno dei più "spinosi". Negli ultimi mesi, infatti, i pirati informatici hanno modificato le loro strategie e sfruttano sempre più spesso il Web per diffondere virus e trojan. La terza edizione di Firefox integra numerosi accorgimenti tecnici per limitare le vulnerabilità sul Web. Tra questi c'è un sistema di controllo che limita la trasmissione dei dati tra diversi siti. Questa operazione di trasmissione, chiamata comunemente Cross-Site, rappresenta infatti uno dei punti deboli che i pirati informatici possono utilizzare per violare le difese del nostro PC.
La nuova versione del browser adotta anche un sistema di controllo delle estensioni installate. Per quanto possano essere utili, infatti, le estensioni sviluppate da programmatori indipendenti rappresentano sempre un potenziale punto debole, soprattutto perché consentono di eseguire aggiunte o modifiche al software. Oltre a controllare periodicamente e automaticamente la disponibilità di aggiornamenti, ora Firefox è in grado di escludere quelli troppo vecchi o che utilizzano un sistema di aggiornamento che può mettere a rischio l'integrità del programma.

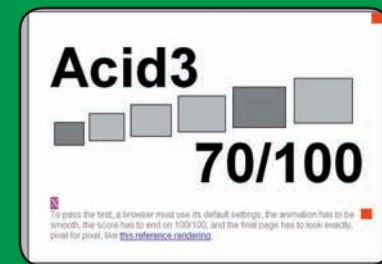
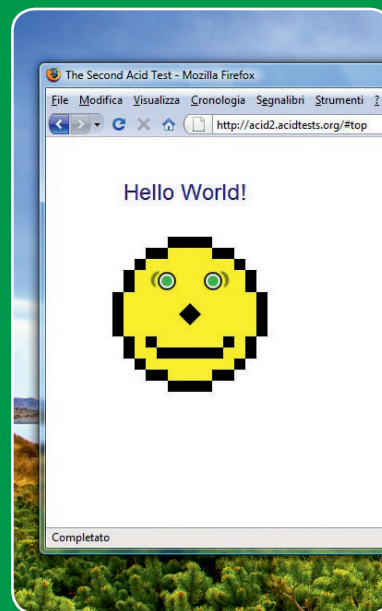
Sempre più spesso, i pirati informatici usano i siti Web per diffondere trojan e virus. Firefox sfrutta una collaborazione con Google per bloccare tempestivamente i siti pericolosi.

:: Controllo dei siti

Con la nuova versione, dunque, la sicurezza del programma è stata migliorata sia sotto il profilo squisitamente tecnico, sia tramite l'integrazione di nuovi strumenti in grado di controllare i siti che visitiamo ed evitare quelli potenzialmente pericolosi.
Il nemico numero uno è il phishing, ovvero i falsi siti Internet simili o identici a quelli di servizi bancari online. In questo caso possiamo affidarci a uno strumento di controllo basato sulla certificazione dei siti, che visualizza una sorta di "sigillo di autenticità" accanto alla barra degli indirizzi.

Una funzione simile ci avvertirà, inoltre, quando stiamo per visualizzare un sito Web che contiene materiale pericoloso, come virus e spyware.

IL TEST ACID

Uno degli elementi attraverso cui è possibile valutare la qualità di un browser è il livello di compatibilità con gli standard Web. Il metodo più diffuso per valutare questo aspetto è il test "Acid". Al momento sono disponibili due versioni del test: Acid 2 e Acid 3. Il nuovo Fiorefox supera a pieni voti il test Acid 2, mentre con Acid 3 ottiene un lusinghiero 70. Sono pochi i browser che possono vantare un punteggio simile nel nuovo, severissimo test.

Il rilevamento e la segnalazione delle pagine Web "a rischio" avviene in collaborazione con Google, che ha da tempo avviato un sistema di monitoraggio del Web per arginare il diffondersi dei virus.

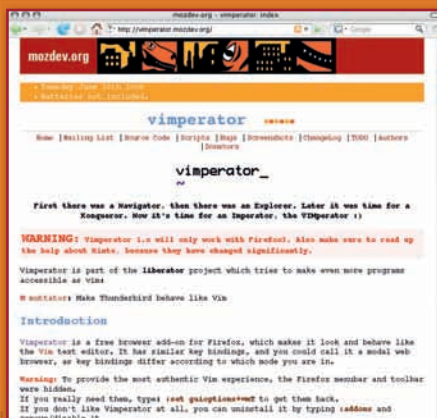
Tutti ONLINE con Vi!

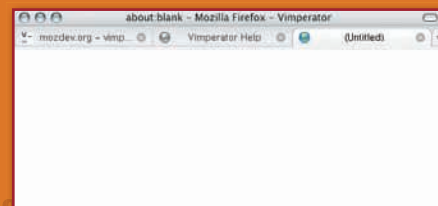
Navigazione, posta e microblogging modale. Per chi ama la linea di comando e gli editor "old sk00l"

Alzi la mano chi non conosce vi! Per quei pochi a cui questa parola non dice nulla chiariamo che si tratta di un famigerato editor da linea di comando (uno dei due) legato a doppio filo alla storia di UNIX.
Vi è il precursore di Wordstar e di Word e di tanti altri ed è noto per la sua versatilità e potenza ma anche per l'usabilità non proprio immediata. Il suo funzionamento a "modi" (in cui separa i comandi dall'editing vero e proprio) è infatti al tempo stesso fonte di frustrazione e di amore da parte degli utenti. Per la gioia di questi ultimi ecco allora alcuni progetti che omaggiano Vi nella sua evoluzione Vim (http://www.vim.org/) adeguando alla sua filosofia d'uso vari programmi e attività su Internet.

:: Il naVimgatore

Tra la miriade di addon e script per Mozilla Firefox ce n'è uno molto particolare che permette di pilotare il browser open source con le combinazioni modali.

Vimperator (http://vimperator.mozdev.org/) è un'aggiunta gratuita per Firefox che ne cambia l'aspetto e il comportamento per adeguarlo all'editor Vim ed ai suoi key bindings.
Al momento in cui scriviamo esistono due versioni di Vimperator, la recente 1.1, rilasciata nel giugno 2008 e rivolta esclusivamente a Firefox 3 e la 0.5.3, del dicembre 2007, rivolta al "vecchio" Firefox 2.

:: Come si usa Vimperator

Una volta installata l'estensione è necessario chiudere e far ripartire Firefox. Al riavvio troveremo il browser estremamente diverso da come ce lo ricordavamo.
Niente menù, aspetto minimale e soprattutto niente barra degli indirizzi. Per fare qualsiasi azione bisogna impostare il comando in maniera corretta.

Ad esempio per aprire un nuovo url e d andare sulla home di Hacker Journal bisogna digitare

```
: open www.hackerjournal.it
```

seguito da invio in quello strano prompt che ora campeggia nella fascia più bassa del browser.
Allo stesso modo per uscire dal software si digiterà :quit

:: Navigazione da tastiera

Gran parte delle operazioni si fanno da linea di comando, come la ricerca su Google per cui digiteremo

```
:open terminecercato
```

Per uscire da questa modalità, come in Vi e Vim si preme il tasto esc

Il mouse -per fortuna- funziona ancora ma chi non vuole "barare" premerà il tasto f con cui a tutti i link verrà associata una scorciatoia e digitando quest'ultima seguita da invio si raggiungerà l'indirizzo. A questo punto con j e k si fa lo scrolling e così via.

Per chi volesse un elenco ed una guida ai comandi basta premere F1 (o digitare <F1>) o visitare il Wiki http://vimperator.cutup.org/index.php?title=Main_Page

:: Muttator: mai più senza

Per chi non ne avesse abbastanza esiste un equivalente per la posta elettronica.

Vimperator è infatti parte di un progetto più ampio chiamato liberator che include anche muttator (http://muttator.mozdev.org/) il cui obiettivo è adeguare anche il mailer Thunderbird ai comandi di Vim ispirandosi (e migliorando, dicono) al programma mutt.
Il motto ironico ma non troppo di muttator "All mail clients suck. Mutt just sucks less. This one just sucks less than Mutt.". Questo perché ciò che si ottiene installandolo è un ambiente leggermente più usabile rispetto all'originale mutt, con più istanze (messaggi, cartelle, ecc.) di posta elettronica in vari tab.

Per l'installazione è necessaria una versione recente di Thunderbird 3 (dalle nightly build) e Vimperator ed è bene sottolineare che .
Anche per questo addon è disponibile un Wiki http://vimperator.cutup.org/index.php?title=Muttator

:: What are you doing? Twitto da Vim

Gli appassionati del servizio di micromessaggistica distribuita Twitter (http://www.twitter.com) che siano anche utenti di Vim possono fare in modo di "twitterare" dal loro editor preferito.

Questo grazie a TwitVim, plugin di Po Shan Cheah (http://www.vim.org/scripts/script.php?script_id=2204) che permette sostanzialmente tutte le operazioni che si fanno da browser, Instant Messenger o client esterno.
Lo script si basa su uno precedente (http://www.vim.org/scripts/script.php?script_id=2124) di Travis Jeffery, anch'esso perfettamente funzionante anche se più semplice nelle funzionalità.

Per l'installazione bisogna prima scaricare lo script, che sarà un file con estensione .vba e poi seguire la procedura descritta sul sito.

Se tutto è andato a buon fine si potrà inviare post da Vim con

```
:PosttoTwitter
```

vedere la timeline con

```
:FriendsTwitter
```

e la propria con

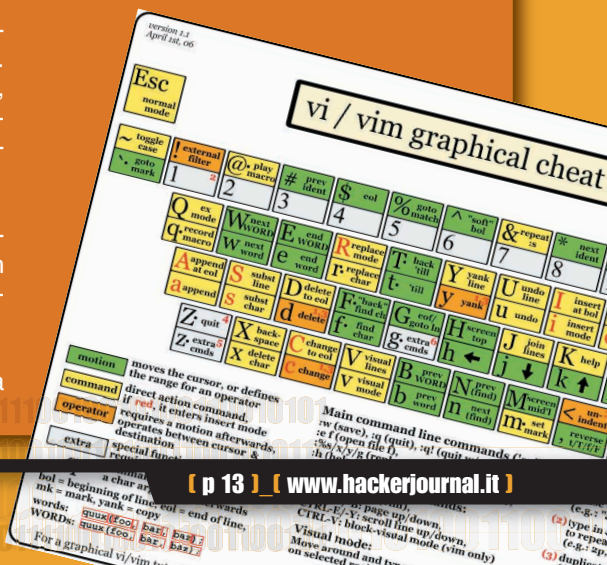
```
:UserTwitter
```

e anche usare funzioni come l'abbreviazione di indirizzi con

```
:Tweetburner
```

e persino fare la ricerca di parole chiave nei messaggi attraverso il servizio Summize con

```
:Summize
```

Nicola D'Agostino

Vecchi sistemi per nuovi hacker

Che la criptologia sia un'arte antica non è un segrete per nessuno ma vediamo come funziona un mistero ancora irrisolto da oltre 200 anni

La leggenda narra che lui si chiamasse Thomas Jefferson Beale e che assieme ad altri 30 amici stesse girando la frontiera a caccia di bufali e avventura, era il 1817. Sembra che la loro caccia sia stata molto più che fortunata e Beale e soci riuscirono a scovare una vena d'oro e una d'argento durante le loro battute e che accumularono un'immensa fortuna che nascosero in un luogo segreto e molto sicuro. Non ancora soddisfatti decisero di partire per nuove avventure ma prima affidarono ad un oste una cassetta contenente la loro storia e tre fogli cifrati dove si spiegava l'entità del tesoro, la sua ubicazione e i nomi dei componenti del gruppo. L'oste avrebbe dovuto aprire la cassetta se entro 10 anni Beale non avesse fatto ritorno e inoltre avrebbe ricevuto la chiave di decriptazione da un altro conoscente di Beale, cosa che gli avrebbe permesso di leggere i messaggi codificati. Gli anni passarono e Beale non fece più ritorno ma all'oste non arrivò neanche mai la chiave e tutt'ora il mistero riguardo il cifrario di Beale e il suo tesoro sono fonte di studi e ricerche.

:: Come funziona

Per prima cosa ricordiamo che le tre pagine codificate da Beale risalgono agli inizi del 1800 ma questo non vuol dire che il suo sistema di codifica sia banale e semplice, in realtà si è servito di un sistema ancora più antico che prevede l'utilizzo di un testo chiave, nel caso del secondo messaggio di Beale, l'unico decodificate, questo chiave è la dichiarazione di indipendenza degli Stati Uniti, ad ogni parola viene associato un numero che però rappresenta solo la prima lettera di quella parola, in questo modo si viene ad avere per la stessa lettera un numero elevato di codici numerici che la rappresentano, facciamo un esempio:

```
1    2       3     4      5  6      7
Nel  mezzo   del   cammin di nostra vita
8  9         10  11  12     13
mi ritrovai  per una selva  oscura
14  15 16       17  18  19
che la diritta via era smarrita...
```

Come possiamo vedere per la lettera N abbiamo solo il numero 1 ma già la M può essere rappresentata con il numero 2 e con l'8 e addirittura la D ha il 3/5/16 in questo modo viene a mancare una delle basi storiche per la decriptazione cioè l'analisi delle sequenze.
Ogni lingua ha alcune lettere, dittongi (coppie di lettere) e parole che vengono ripetute più spesso di altre e anche le lettere iniziali delle parole sono valutabili in percentuali abbastanza precise, in questo modo un decodificatore può permettersi di azzardare alcune ipotesi aprioristiche basate sulle sequenze e poi di confermarle. L'utilizzo del sistema utilizzato da Beale fa in modo che le sequenze vadano a sparire visto che per la stessa lettera possono essere utilizzati diversi numeri. L'unico modo per decodificare un messaggio di questo tipo è avere la chiave.

71, 194, 38, 1701, 89, 76, 11, 83, 1629, 48, 94, 63, 132, 16, 111, 95, 84, 341, 975,
14, 40, 64, 27, 81, 139, 213, 63, 90, 1120, 8, 15, 3, 126, 2018, 40, 74, 758, 485,
604, 230, 436, 664, 582, 150, 251, 284, 308, 231, 124, 211, 486, 225, 401, 370,
11, 101, 305, 139, 189, 17, 33, 88, 208, 193, 145, 1, 94, 73, 416, 918, 263, 28, 500,
538, 356, 117, 136, 219, 27, 176, 130, 10, 460, 25, 485, 18, 436, 65, 84, 200, 283,
118, 320, 138, 36, 416, 280, 15, 71, 224, 961, 44, 16, 401, 39, 88, 61, 304, 12, 21,
24, 283, 134, 92, 63, 246, 486, 682, 7, 219, 184, 360, 780, 18, 64, 463, 474, 131,
160, 79, 73, 440, 95, 18, 64, 581, 34, 69, 128, 367, 460, 17, 81, 12, 103, 820, 62,
116, 97, 103, 862, 70, 60, 1317, 471, 540, 208, 121, 890, 346, 36, 150, 59, 568,
614, 13, 120, 63, 219, 812, 2160, 1780, 99, 35, 18, 21, 136, 872, 15, 28, 170, 88, 4,
30, 44, 112, 18, 147, 436, 195, 320, 37, 122, 113, 6, 140, 8, 120, 305, 42, 58, 461,
44, 106, 301, 13, 408, 680, 93, 86, 116, 530, 82, 568, 9, 102, 38, 416, 89, 71, 216,
728, 965, 818, 2, 38, 121, 195, 14, 326, 148, 234, 18, 55, 131, 234, 361, 824, 5,
81, 623, 48, 961, 19, 26, 33, 10, 1101, 365, 92, 88, 181, 275, 346, 201, 206, 86,
36, 219, 324, 829, 840, 64, 326, 19, 48, 122, 85, 216, 284, 919, 861, 326, 985,
233, 64, 68, 232, 431, 960, 50, 29, 81, 216, 321, 603, 14, 612, 81, 360, 36, 51, 62,
194, 78, 60, 200, 314, 676, 112, 4, 28, 18, 61, 136, 247, 819, 921, 1060, 464, 895,
10, 6, 66, 119, 38, 41, 49, 602, 423, 962, 302, 294, 875, 78, 14, 23, 111, 109, 62,
31, 501, 823, 216, 280, 34, 24, 150, 1000, 162, 286, 19, 21, 17, 340, 19, 242, 31,
86, 234, 140, 607, 115, 33, 191, 67, 104, 86, 52, 88, 16, 80, 121, 67, 95, 122, 216,
548, 96, 11, 201, 77, 364, 218, 65, 667, 890, 236, 154, 211, 10, 98, 34, 119, 56,
216, 119, 71, 218, 1164, 1496, 1817, 51, 39, 210, 36, 3, 19, 540, 232, 22, 141, 617,
84, 290, 80, 46, 207, 411, 150, 29, 38, 46, 172, 85, 194, 39, 261, 543, 897, 624, 18,
212, 416, 127, 931, 19, 4, 63, 96, 12, 101, 418, 16, 140, 230, 460, 538, 19, 27, 88,
612, 1431, 90, 716, 275, 74, 83, 11, 426, 89, 72, 84, 1300, 1706, 814, 221, 132,
40, 102, 34, 868, 975, 1101, 84, 16, 79, 23, 16, 81, 122, 324, 403, 912, 227, 936,
447, 55, 86, 34, 43, 212, 107, 96, 314, 264, 1065, 323, 428, 601, 203, 124, 95, 216,
814, 2906, 654, 820, 2, 301, 112, 176, 213, 71, 87, 96, 202, 35, 10, 2, 41, 17, 84,
221, 736, 820, 214, 11, 60, 760.

Ecco la pagina di codice che racconta il dove si trova il tesoro

:: La seconda pagina

Qui di seguito vi riportiamo la decodifica (tradotta in italiano) della seconda pagina del Cifrario, leggendo quello che Beale dice di aver nascosto si può anche capire perché la gente continui a cercare di risolvere questo mistero.

« Ho depositato nel paese di Bedford a circa 4 miglia da Bufords in una fossa o in una cripta 6 piedi sottoterra, i seguenti articoli che appartengono al gruppo di persone i cui nomi sono nell'allegato "3". Il primo deposito è consistito in 1.014 libbre d'oro e 38.012 libbre di argento, depositate nel novembre del 1819. Il secondo è stato fatto nel dicembre del 1821 ed è consistito da 38007 libbre di oro e 12018 libbre d'argento, e anche gioielli ottenuti a St. Louis per ridurre la fatica nel trasporto, valutati 13.000 dollari. Quanto sopra è nascosto al sicuro in recipienti di ferro con coperchi sempre di ferro. La fossa è malemente coperta dalla pietra e gli altri recipienti sono collocati sulla solida pietra e sono coperti da altre (pietre). Il foglio numero uno descrive l'esatta località della fossa così non sarà complicato a trovarla. »

115, 73, 24, 807, 37, 52, 49, 17, 31, 62, 647, 22, 7, 15, 140, 47, 29, 107, 79, 84, 56,
239, 10, 26, 811, 5, 196, 308, 85, 52, 160, 136, 59, 211, 36, 9, 46, 316, 554, 122,
106, 95, 53, 58, 2, 42, 7, 35, 122, 53, 31, 82, 77, 250, 196, 56, 96, 118, 71, 140,
287, 28, 353, 37, 1005, 65, 147, 807, 24, 3, 8, 12, 47, 43, 59, 807, 45, 316, 101, 41,
78, 154, 1005, 122, 138, 191, 16, 77, 49, 102, 57, 72, 34, 73, 85, 35, 371, 59, 196,
81, 92, 191, 106, 273, 60, 394, 620, 270, 220, 106, 388, 287, 63, 3, 191, 122, 43,
234, 400, 106, 290, 314, 47, 48, 81, 96, 26, 115, 92, 158, 191, 110, 77, 85, 197, 46,
10, 113, 140, 353, 48, 120, 106, 2, 607, 61, 420, 811, 29, 125, 14, 20, 37, 105, 28,
248, 16, 159, 7, 35, 19, 301, 125, 110, 486, 287, 98, 117, 511, 62, 51, 220, 37, 113,
140, 807, 138, 540, 8, 44, 287, 388, 117, 18, 79, 344, 34, 20, 59, 511, 548, 107,
603, 220, 7, 66, 154, 41, 20, 50, 6, 575, 122, 154, 248, 110, 61, 52, 33, 30, 5, 38, 8,
14, 84, 57, 540, 217, 115, 71, 29, 84, 63, 43, 131, 29, 138, 47, 73, 239, 540, 52, 53,
79, 118, 51, 44, 63, 196, 12, 239, 112, 3, 49, 79, 353, 105, 56, 371, 557, 211, 515,
125, 360, 133, 143, 101, 15, 284, 540, 252, 14, 205, 140, 344, 26, 811, 138, 115,
48, 73, 34, 205, 316, 607, 63, 220, 7, 52, 150, 44, 52, 16, 40, 37, 158, 807, 37, 121,
12, 95, 10, 15, 35, 12, 131, 62, 115, 102, 807, 49, 53, 135, 138, 30, 31, 62, 67, 41,
85, 63, 10, 106, 807, 138, 8, 113, 20, 32, 33, 37, 353, 287, 140, 47, 85, 50, 37, 49,
47, 64, 6, 7, 71, 33, 4, 43, 47, 63, 1, 27, 600, 208, 230, 15, 191, 246, 85, 94, 511, 2,
270, 20, 39, 7, 33, 44, 22, 40, 7, 10, 3, 811, 106, 44, 486, 230, 353, 211, 200, 31,
10, 38, 140, 297, 61, 603, 320, 302, 666, 287, 2, 44, 33, 32, 511, 548, 10, 6, 250,
557, 246, 53, 37, 52, 83, 47, 320, 38, 33, 807, 7, 44, 30, 31, 250, 10, 15, 35, 106,
160, 113, 31, 102, 406, 230, 540, 320, 29, 66, 33, 101, 807, 138, 301, 316, 353,
320, 220, 37, 52, 28, 540, 320, 33, 8, 48, 107, 50, 811, 7, 2, 113, 73, 16, 125, 11,
110, 67, 102, 807, 33, 59, 81, 158, 38, 43, 581, 138, 19, 85, 400, 38, 43, 77, 14, 27,
8, 47, 138, 63, 140, 44, 35, 22, 177, 106, 250, 314, 217, 2, 10, 7, 1005, 4, 20, 25,
44, 48, 7, 26, 46, 110, 230, 807, 191, 34, 112, 147, 44, 110, 121, 125, 96, 41, 51,
50, 140, 56, 47, 152, 540, 63, 807, 28, 42, 250, 138, 582, 98, 643, 32, 107, 140,
112, 26, 85, 138, 540, 53, 20, 125, 371, 38, 36, 10, 52, 118, 136, 102, 420, 150,
112, 71, 14, 20, 7, 24, 18, 12, 807, 37, 67, 110, 62, 33, 21, 95, 220, 511, 102, 811,
30, 83, 84, 305, 620, 15, 2, 108, 220, 106, 353, 105, 106, 60, 275, 72, 8, 50, 205,
185, 112, 125, 540, 65, 106, 807, 188, 96, 110, 16, 73, 33, 807, 150, 409, 400, 50.

Questa è l'unica pagina decodificata del Cifrario di Beale e descrive il tesoro

317, 8, 92, 73, 112, 89, 67, 318, 28, 96, 107, 41, 631, 78, 146, 397, 118, 98, 114,
246, 348, 116, 74, 88, 12, 65, 32, 14, 81, 19, 76, 121, 216, 85, 33, 66, 15, 108, 68,
77, 43, 24, 122, 96, 117, 36, 211, 301, 15, 44, 11, 46, 89, 18, 136, 68, 317, 28, 90,
82, 304, 71, 43, 221, 198, 176, 310, 319, 81, 99, 264, 380, 56, 37, 319, 2, 44, 53,
28, 44, 75, 98, 102, 37, 85, 107, 117, 64, 88, 136, 48, 154, 99, 175, 89, 315, 326,
78, 96, 214, 218, 311, 43, 89, 51, 90, 75, 128, 96, 33, 28, 103, 84, 65, 26, 41, 246,
84, 270, 98, 116, 32, 59, 74, 66, 69, 240, 15, 8, 121, 20, 77, 89, 31, 11, 106, 81,
191, 224, 328, 18, 75, 52, 82, 117, 201, 39, 23, 217, 27, 21, 84, 35, 54, 109, 128,
49, 77, 88, 1, 81, 217, 64, 55, 83, 116, 251, 269, 311, 96, 54, 32, 120, 18, 132, 102,
219, 211, 84, 150, 219, 275, 312, 64, 10, 106, 87, 75, 47, 21, 29, 37, 81, 44, 18,
126, 115, 132, 160, 181, 203, 76, 81, 299, 314, 337, 351, 96, 11, 28, 97, 318, 238,
106, 24, 93, 3, 19, 17, 26, 60, 73, 88, 14, 126, 138, 234, 286, 297, 321, 365, 264,
19, 22, 84, 56, 107, 98, 123, 111, 214, 136, 7, 33, 45, 40, 13, 28, 46, 42, 107, 196,
227, 344, 198, 203, 247, 116, 19, 8, 212, 230, 31, 6, 328, 65, 48, 52, 59, 41, 122,
33, 117, 11, 18, 25, 71, 36, 45, 83, 76, 89, 92, 31, 65, 70, 83, 96, 27, 33, 44, 50, 61,
24, 112, 136, 149, 176, 180, 194, 143, 171, 205, 296, 87, 12, 44, 51, 89, 98, 34, 41,
208, 173, 66, 9, 35, 16, 95, 8, 113, 175, 90, 56, 203, 19, 177, 183, 206, 157, 200,
218, 260, 291, 305, 618, 951, 320, 18, 124, 78, 65, 19, 32, 124, 48, 53, 57, 84, 96,
207, 244, 66, 82, 119, 71, 11, 86, 77, 213, 54, 82, 316, 245, 303, 86, 97, 106, 212,
18, 37, 15, 81, 89, 16, 7, 81, 39, 96, 14, 43, 216, 118, 29, 55, 109, 136, 172, 213,
64, 8, 227, 304, 611, 221, 364, 819, 375, 128, 296, 1, 18, 53, 76, 10, 15, 23, 19, 71,
84, 120, 134, 66, 73, 89, 96, 230, 48, 77, 26, 101, 127, 936, 218, 439, 178, 171, 61,
226, 313, 215, 102, 18, 167, 262, 114, 218, 66, 59, 48, 27, 19, 13, 82, 48, 162, 119,
34, 127, 139, 34, 128, 129, 74, 63, 120, 11, 54, 61, 73, 92, 180, 66, 75, 101, 124,
265, 89, 96, 126, 274, 896, 917, 434, 461, 235, 890, 312, 413, 328, 381, 96, 105,
217, 66, 118, 22, 77, 64, 42, 12, 7, 55, 24, 83, 67, 97, 109, 121, 135, 181, 203, 219,
228, 256, 21, 34, 77, 319, 374, 382, 675, 684, 717, 864, 203, 4, 18, 92, 16, 63, 82,
22, 46, 55, 69, 74, 112, 134, 186, 175, 119, 213, 416, 312, 343, 264, 119, 186, 218,
343, 417, 845, 951, 124, 209, 49, 617, 856, 924, 936, 72, 19, 28, 11, 35, 42, 40, 66,
85, 94, 112, 65, 82, 115, 119, 236, 244, 186, 172, 112, 85, 6, 56, 38, 44, 85, 72,
32, 47, 73, 96, 124, 217, 314, 319, 221, 644, 817, 821, 934, 922, 416, 975, 10, 22,
18, 46, 137, 181, 101, 39, 86, 103, 116, 138, 164, 212, 218, 296, 815, 380, 412,
460, 495, 675, 820, 952.

La terza pagina del messaggio parla dei soci di Beale

:: La sfida

Vorremmo proporvi qui di fila 2 indovinelli basati sul sistema di codifica usato da Beale.

Il primo sarà a chiave unica, quindi un testo di riferimento utilizzato come Beale ha utilizzato la dichiarazione di indipendenza per il suo secondo messaggio

Il secondo sarà a doppia chiave, quindi il messaggio cifrato sarò in lettere alle quali corrispondono i numeri codificati di un primo testo chiave che a loro volta corrispondono alle lettere del secondo testo chiave, facciamo un esempio

```
1        2      3    4    5    6
Respiri piano per non far rumore
7  8            9   10    11
Ti addormenti di sera e
12  13       14   15
ti  risvegli col sole
16  17      18    19
Sei chiara come l'alba,
20  21      22    23
Sei fresca come l'aria


1         2        3  4
Generale dietro la collina
5  6   7  8      9       10  11
Ci sta la notte crucca ed assassina
12 13 14    15   16    1718 19   20
E  in mezzo al  prato c'è una contadina
```

Soluzione: PRESA
Prima codifica A (Alba Chiara):
2 6 11 10 8
Seconda codifica B (Generale):
D S A E N

SE PROPRIO NON RIUSCITE

Nel nuovo blog dedicato ad HJ bigg- theguilty@blogspot.com abbiamo caricato i testi chiave da cui potrete partire per decodificare i due messaggi oggetti del nostro quiz.

Ed ecco quindi i due testi codificati e gli indovinelli per capire i testi chiave, buon divertimento

Enigma 1: 8 2 11 54 / 46 17 1 100 / 15 18 67 79 66 100
Quiz per la chiave: Triste se ne sta su una collina al tramonto il felino poeta che ammira ciò che non ha limite.

Enigma 2: L S D / C P S / A Q E / E S D H / D L S D E N E E

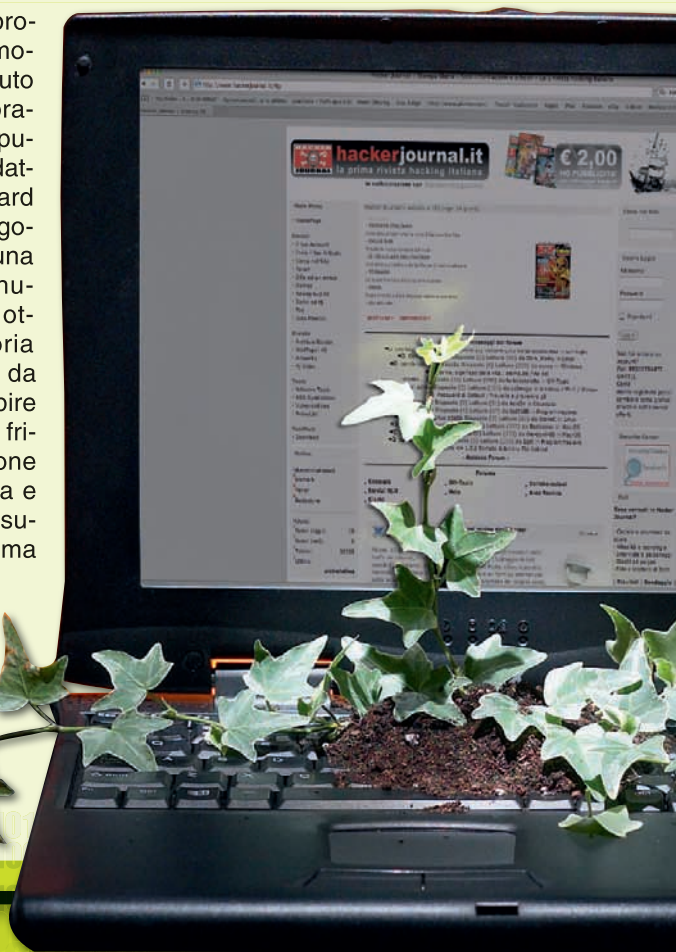
Quiz per la chiave A: Ha vinto un nobel parlando in italiano di ossa di molluschi, in questo caso a mezzogiorno riflette vicino ad un rovente muro

Quiz per la chiave B: Il sommo poeta che è sceso all'inferno e che scrive parole dure come pietra quando ormai resta poco giorno e le ombre si allungano.

BigG

Un COMPUTER più verde

Un approccio ragionato alla scelta dei componenti ci può consentire di aver un computer altrettanto potente ma con un minor impatto ambientale. Gli strumenti elettronici e informatici hanno infatti un legame molto più stretto di quanto normalmente si creda con l'ecologia...

Nella classifica delle questioni globali sulla bocca di tutti, l'effetto serra è sicuramente ai primi posti. Si tratta di un fenomeno per cui le emissioni di anidride carbonica, intrappolando il calore all'interno della nostra atmosfera, determinano un innalzamento progressivo della temperatura nel globo che ha conseguenze nefaste sull'ambiente. I ghiacciai si riducono a velocità senza precedenti, le calotte polari si sciolgono con gravi danni sulla fauna (sono documentati casi di orsi polari affogati perché non ci sono più sufficienti piattaforme di ghiaccio...) e sull'ecosistema. Cosa c'entriamo noi? Beh, anche se non siamo responsabili quanto fabbriche, impianti per la produzione di energia e automobili, diamo il nostro contributo con i computer. Può sembrare inverosimile ma un computer dotato di componenti adatti al gioco in 3D agli standard attuali consuma più di un frigorifero. Un PC veloce con una scheda grafica potente, numerosi hard disk e unità ottiche, un lettore di memoria flash e uno schermo LCD da 30 pollici può infatti assorbire 750 watt, contro i 725 di un frigorifero medio. La situazione non è sempre così drastica e in media un computer consuma tra i 200 e i 400 watt, ma se pensiamo che un televisore ne assorbe circa 100 e un lettore di DVD 25 ci renderemo conto che c'è ampio spazio per il miglioramento. A trarne beneficio non sarà solo il pianeta ma

anche il nostro portafoglio, perché eviteremo bollette esorbitanti per il consumo elettrico.

:: Caccia ai componenti

All'interno del nostro computer, i primi responsabili del consumo energetico sono la CPU e la scheda grafica. Anche se i produttori, in genere, sono sempre più sensibili al problema, una Core 2 Duo Extreme di Intel assorbe 75 watt, che non sono pochi, e una scheda di buona potenza, come i modelli di ATI o nVidia, può portare il consumo della nostra macchina oltre i 300 watt. Un altro vampiro di energia è il monitor a tubo catodico, che può assorbire fino a 100 watt. Sono tutti questi elementi che ci portano spesso a dover prendere degli alimentatori più potenti (come dicevamo, anche da 750 watt) e questi a loro volta consumano energia... Dovremo quindi rinunciare al computer o ai videogiochi in nome dell'ecologia? Nessuno invoca una soluzione così radicale. Scegliendo bene i componenti, però, potremo avere un computer più verde a parità di potenza.

:: Scelte ponderate

Il segreto per riuscire ad assemblare una macchina che bilanci prestazioni e impatto ambientale consiste nel leggere attentamente le specifiche e cercare componenti tecnologicamente avanzati ma con un occhio di riguardo ai consumi. Per esempio il Core 2 Duo E6700 di Intel è notevolmente più veloce di un Pentium D 960 (circa il 40%) e consuma il 40% in meno. Possiamo abbinarlo a una scheda madre DG965SS di Intel che non solo ha un basso consumo (20

LA MELA NON E' ABBASTANZA VERDE

L'impatto dei prodotti elettronici e del computer sull'ambiente non è sfuggito agli ecologisti. Per esempio, Greenpeace è molto interessata all'argomento (diamo un'occhiata al sito greenpeace.org/electronics) e dall'agosto del 2006 pubblica una classifica (aggiornata ogni tre mesi) dei principali produttori del mondo in base alla loro "ecologicità". I criteri presi in considerazione si suddividono principalmente in due categorie: utilizzo di materiali tossici nel processo produttivo e politica di ritiro e riciclo dei dispositivi divenuti obsoleti. Alle aziende vengono attribuiti dei voti dallo 0 al 10 sulla base di questi parametri. La versione del marzo 2008 (che troviamo all'indirizzo http://www.greenpeace.org/international/campaigns/toxics/electronics/how-the-companies-line-up o, in italiano, http://www.greenpeace.org/italy/campagne/inquinamento/hi-tech/ecoguida) vede al primo posto per impegno ambientalistico a pari merito Samsung e Toshiba con un punteggio di 7,7. La prima vede la sua posizione brillare per le politiche di utilizzo delle sostanze tossiche mentre la seconda spicca dal punto di vista della gestione dei prodotti ormai superati. Seguono (con un punteggio di 7,3) Nokia, Sony, Dell e Lenovo. Sempre in lizza per arrivare a essere considerate aziende verdi ma un po' più indietro, con punteggi che vanno dal 6,3 al 6,7, troviamo Sony Ericsson, LGE, Apple, Fujitsu-Siemens, HP e Motorola. Se ci sorprende notare che il produttore dei computer Macintosh, tradizionalmente i più amati negli ambienti alternativi associati all'ecologia, non sia tra le aziende più impegnate su questo fronte, ci stupirà ancora di più sapere che questa posizione è il frutto di un notevole miglioramento: nella prima classifica aveva un tristissimo punteggio di 2,7 ed era mal valutato praticamente sotto tutti i punti di vista. Greenpeace ha in atto una campagna specifica per sensibilizzare l'azienda sulle tematiche ecologiste (http://www.greenmyapple.org/it/). In questa edizione delle ecoclassifica, comunque, il fanalino di coda è Nintendo, con un misero 0,3. A questo proposito, sul sito italiano di Greenpeace troviamo anche una campagna sulle console di gioco (http://www.greenpeace.it/console/).

watt) ma ha anche una scheda grafica 3D integrata che ci permette di evitare (a meno che non usiamo il computer per giocare con i titoli più recenti) l'installazione di un componente aggiuntivo. Anche AMD produce delle CPU a basso consumo, la serie X2, che comprende modelli interessanti anche dal punto di vista del prezzo d'acquisto. Se la scheda grafica integrata nella scheda madre o nella CPU non basta a coprire le nostre esigenze perché siamo appassionati di videogiochi, dovremo fare una scelta. Potremo avere una scheda potentissima e rinunciare ai bassi consumi energetici (attualmente questi due fattori sono proprio inconciliabili) oppure orientarci su un modello di media potenza. Per esempio la GeForce 7900gs consuma 20W "a riposo" e 50W quando lavora, la Radeon 1950Pro passa da 24W a 64W e la 8800gts richiede 55W di base e 102W sotto carico. CPU e scheda grafica non sono i soli elementi da tenere in considerazione.
Per esempio, un disco fisso SATA consuma un po' meno di un IDE e i modelli a singolo piatto sono preferibili a quelli a doppio piatto sotto questo profilo. Diamo un'occhiata anche alle caratteristiche del sistema di raffreddamento e del case: adottiamone uno leggero con un buon sistema di aerazione che limiti l'impegno delle ventole. Persino la scelta dell'alimentatore può aiutarci a risparmiare energia: optiamo per un modello conforme con lo standard 80 plus (vedi box). Se alcuni componenti non ci permettono di usare Windows Vista, possiamo orientarci su Ubuntu o un altro sistema operativo gratuito della famiglia di Linux. Otterremo così prestazioni equivalenti sfruttando meno risorse di sistema.

:: Non solo consumi

Se il risparmio energetico è una considerazione primaria nella scelta di un computer verde, non bisogna dimenticare le tecniche produttive.
Le saldature di schede madri, processori e altri componenti sono in genere fatte in piombo, il cui smaltimento crea dei residui tossici. Nella produzione dei monitor a tubo catodico, inoltre, vengono impiegati materiali tossici come piombo, mercurio, bario, cadmio e fosforo. Ai prodotti fabbricati o importati in Europa si applica la Direttiva RoHS (dall'inglese: Restriction of Hazardous Substances Directive) adottata nel febbraio del 2003 dalla Comunità Europea e nota anche con il nome ufficiale di normativa 2002/95/CE. Impone restrizioni sull'uso di determinate sostanze (tra cui piombo,

L'IMPORTANZA DELLA GIUSTA ALIMENTAZIONE

Può sembrare bizzarro, ma l'ottimizzazione dei consumi non è tra gli obiettivi principali di tutti gli alimentatori per computer. Spesso infatti si sovraalimentano quando sono usati al di sotto del massimo carico, ai danni della nostra bolletta e dell'ambiente. C'è però un modo per verificare che il nostro alimentatore opti per un consumo ragionato: il programma 80 Plus. Si tratta di un sistema di certificazione volontario adottato da un gruppo di produttori. Per poter essere certificato 80 Plus un alimentatore deve essere "verde" sotto vari aspetti: non deve contenere piombo, deve rispettare la normativa RoHS (vedi sopra) e deve assorbire solo l'elettricità necessaria alle esigenze del nostro computer in quel momento. Se, per esempio, abbiamo un alimentatore da 750 watt perché abbiamo montato una seconda scheda grafica super potente, la piena potenza dell'alimentatore sarà assorbita solo quando la sfruttiamo. Se, per esempio, mentre lavoriamo con un elaboratore di testi l'energia necessaria al computer è del 20% di quella assorbita al massimo carico, il nostro alimentatore fornirà al sistema solo 150 watt. Il funzionamento di questa autoregolazione è analogo a quello di un impianto di riscaldamento regolato da termostato: invece di avere i caloriferi che vanno sempre alla massima potenza facendoci morire di caldo nelle giornate più temperate, abbiamo un sensore di temperatura che mantiene la nostra casa sempre a 21 gradi, senza sprechi. Adottare un alimentatore 80 Plus sul nostro computer ci permette di salvare circa 85 kilowatt/ora all'anno per macchina. Un risparmio sensibile sia in termini economici che ambientali e un modo per dire grazie alle aziende che si preoccupano di più del futuro del pianeta. Per saperne di più visitiamo il sito www.80plus.org.

mercurio, cadmio e cromo esavalente) nella costruzione di vari tipi di apparecchiature elettriche ed elettroniche. Anche la rottamazione di questi prodotti è soggetta a una normativa europea, la direttiva WEEE (dall'inglese Waste Electrical and Electronic Equipment), o norma 2002/96/CE, più nota in Italia come direttiva RAEE (da Rifiuti di apparecchiature elettriche ed elettroniche). La direttiva mira a limitare i problemi legati all'accumulo di apparecchiature elettroniche di scarto nelle discariche.

Contenendo sostanze, tossiche infatti, non devono essere trattate come gli altri rifiuti (bruciarli porterebbe a disperdere nell'ambiente sostanze nocive) ma vanno trattate specificamente mirando al massimo riciclo dei materiali.

Lo sforzo legislativo è incoraggiante ma non è presente negli Stati Uniti (con l'eccezione della California che ha varato norme equivalenti) e alcuni produttori, secondo una ricerca condotta da Greenpeace, sembrano infischiarsene allegramente di ogni conseguenza ecologica.

Nell'assemblare il nostro computer, ma anche nel scegliere il cellulare o qualsiasi dispositivo elettrico o elettronico, proviamo a considerare non solo l'aspetto estetico, le prestazioni e il costo d'acquisto ma anche i consumi e l'impatto ambientale delle politiche dell'azienda.

Daremo il nostro contributo per un pianeta più verde...

Come ti CRACKO il GSM

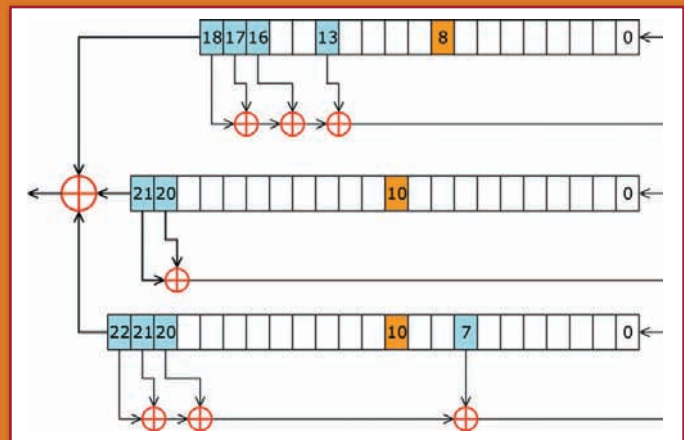
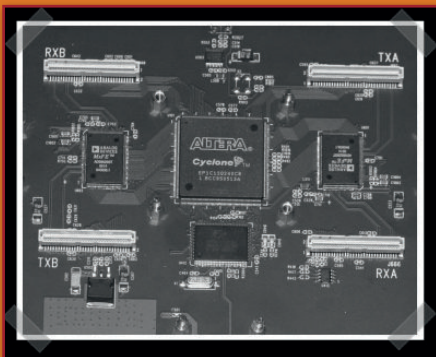
Pochi ne parlano ma vogliamo dimostrarvi come le nostre comunicazioni sono veramente poco sicure, 1.000 euro e tutti possono ascoltare il nostro cellulare

Mentre sto scrivendo, il wiki relativo al crack del gsm (wiki.thc.org/cracking_a5) non è più disponibile online ed è visibile solo nella cache di google. Forse queste informazioni disponibili a tutti danno fastidio a qualcuno. Infatti il progetto fa riferimento alla possibilità di realizzare un kit elettronico del costo di 1000 dollari (640 euro al cambio attuale) in grado di rompere le difese di sicurezza del protocollo gsm e permettere quindi di decrittare una telefonata che per sua natura è cifrata e resa intellegibile solo ai sistemi elettronici dei gestori coinvolti durante la conversazione, dopo circa 30-60 minuti. L'obiettivo finale è quello di ridurre questo tempo a 30 secondi (o meno) facendo uso di un hardware meno costoso di quello usato dalle varie intelligence (1-2 milioni di dollari nel 2001). Il kit si basa su una falla relativa alla codifica A5 già scoperta nel 1994 e approfondita da diversi documenti accademici che non è stata chiusa, ma solo arginata in quanto parte integrante del sistema gsm. Ma invece di denunciarlo, i gestori mobili insistono nel dire che le comunicazioni gsm sono le più sicure al mondo quando risulta ad esempio che in Russia e Ucraina, durante le emergenze (che possono essere anche molto lunghe) vengono disabilitate completamente le codifiche, mentre in alcuni paesi arabi non sono attive per niente. Non solo: sembra che una qualunque antenna per cellulari (la BTS) sovraccarica di chiamate possa disattivare la protezione sulle comunicazioni in transito. La situazione è potenzialmente molto grave: sniffando il traffico e registrandolo, è possibile decodificarlo in seguito e mettere in chiaro quindi anche comunicazioni avute nel passato. Per capire di cosa stiamo parlando bisogna chiarire che cos'è l'A5. L'A5 è un algoritmo che si basa su chiavi di crittazione usate per la trasmissione dei pacchetti di bit (burst) in cui viene scomposta la comunicazione via gsm (sia essa voce o dati/sms), che è stato

	Come codificare il messaggio GSM
1	23 * 8 = 184 bit di dati contenuti per messaggio GSM. [Output: 184 bit]
2	Aggiungi 40 bit fire code (crc) e 4 bit in coda (0x00). [Output: 228 bit]
3	Codifica tramite convoluzione i 228 bit. Questo duplica il numero dei bit (conosciuti). [Output: 456 bit]
4	Esegui l'interleave dei 456 bit. [Output: 456 bit]
5	Taglia i 456 bit in 8 pacchetti, ognuno lungo 57 bit. Prendi i primi due pacchetti da 57 bit e mandali nel primo GSM burst. Il 3o e il 4o vengono spediti nel secondo GSM burst e così via. [Output: 4x114 bit]
6	Il numero di frame è conosciuto e incrementato per ogni GSM burst. A5 viene reinizializzato per OGNI burst. Questo significa che ogni burst è codificato con lo stesso Kc ma con un diverso numero di frame. Lo stato di A5 state è quindi diverso per ogni GSM burst.

* Il numero di frame (FN) viene azzerato all'incirca ogni 3 ore, 28 minuti, 53 secondi e 750 millisecondi
* Un messaggio GSM è lungo 23 ottetti (1 ottetto = 1 byte)

bucato nel 1994 e completamente aperto nel 1999 (en.wikipedia.org/wiki/A5/1). Nel 1987, quando ancora l'A5 era tenuto completamente segreto, venne sviluppato l'A5/1 allo scopo di fortificare un algoritmo di protezione che iniziava ad essere richiesto al di fuori dell'Europa (leggi NATO). Per questi nuovi richiedenti, venne realizzata una versione indebolita dell'algoritmo, la A5/2, ma ad oggi quasi tutti i gestori adottano l'A5/1 o il nuovo A5/3 (detto KASUMI) introdotto per le reti 3G e anch'esso oggetto di studio (e attacchi). Ma si tratta sempre di varianti dello stesso algoritmo insicuro e per il quale ogni tanto un gruppo indipendente o un diverso professore universitario propongono un metodo di crack nuovo! In Tabella 1 si vede un esempio di applicazione dell'algoritmo A5. Per il crack, la chiave di volta risiede nell'uso della FPGA, un dispositivo hardware riprogrammabile che permette di essere riconfigurato all'infinito al fine di realizzare gli elementi di una rete logica senza averli fisicamente, ma con le prestazioni analoghe a quelle che si avrebbero realmente. Attraverso l'uso di più FPGA in parallelo si riesce a emulare dopo alcuni cicli il processo di crittazione in corso durante una telefonata cellulare. In pratica si fa uso di un brute force evoluto che mettendo in parallelo processori dedicati realizzati all'interno della FPGA riesce a clonare le chiavi alla base dell'algoritmo A5 e quindi rende possibile la decrittazione della telefonata (o dell'sms). In particolare esistono diversi metodi che permettono di diminuire la durata di questo processo, in cui la variabile principale è essenzialmente il costo. Infatti già nel 2001 veniva pubblicato uno studio che basava l'attacco bruto sull'uso di 1000 FPGA in parallelo (pv.fernuni-hagen.de/docs/apc2001-final.pdf), mentre oggi con una sola FPGA LX50 occorrono 30-60 minuti e con 32 FPGA (A5 Buster) si scende ai 30 secondi proposti dal progetto. C'è da dire che oltre alle FPGA occorre anche una discreto spazio di lavoro: si parla di 2-4 Terabyte di hard-drive (o flash)! Ma chiaramente, nulla vieta di realizzare un servizio di crack disponibile online: si inviano i burst per la decrittazione al server remoto e nel giro di qualche secondo si riceve indietro la chiave in chiaro per decodificare la chiamata. E può capitare che nonostante la rete in uso adotti la protezione migliore, in realtà sms o chiamate non vengano comunque crittate e viaggino in chiaro. Al di là dei discorsi legati alle intercettazioni e alla privacy, per scoprire se il proprio operatore e in particolare se le antenne sulle quali il nostro cellulare sta girando le nostre comunicazioni, stanno utilizzando la protezione A5/1 o meno, possiamo utilizzare il famoso NetMonitor e un telefono Nokia con symbian o anche un vecchio telefono basato su DCT3 (come il Nokia 3310) più Gammu (www.gammu.org) e un pc. Per NetMonitor la procedura è la seguente: 1) assicurarsi di essere su network GSM 2) installare NetMonitor collegando il telefono al pc via cavo usb e lanciarlo 3) andare sulla schermata 1.10; 4) spedire chiamare il telefono (o mandargli un sms) e verificare se 'Ciphering val' cambia da OFF a qualcos'altro (A51 o A52). Se rimane a OFF non c'è alcuna protezione attiva! Resta che A5/1 e A5/2 sono obsoleti da 14 anni e A5/3 è insicuro già da 3 anni (en.wikipedia.org/wiki/A5/3).

Massimiliano Brasile

UBUNTU e PS3 come media server

Perché dovremmo limitarci ad avere il controllo sui nostri computer quando potremmo ampliare la nostra rete con console come la PS3 e l'X-box?

Una rete che si estende a tutta la casa e fuori, con computer, dispositivi portatili, console e altri strumenti elettronici tutti collegati e interattivi... fino a qualche anno fa sembrava fantascienza ma è sempre più realizzabile, anche grazie alla diffusione dello standard DLNA. Questa sigla sta per Digital Living Network Alliance e indica un gruppo fondato nel 2003 con lo scopo di incoraggiare il maggior numero di produttori possibile ad abbracciare uno standard aperto che permetta la condivisione di file multimediali sui supporti più disparati attraverso una rete cablata o wireless. L'idea è evidentemente brillante ma ci saremmo aspettati che i colossi dell'industria opponessero un secco "no" all'idea di avere milioni di persone che mettono le mani nei loro preziosi dispositivi. Così non è stato: sono più di 250 le aziende che hanno abbracciato il DLNA e includono giganti come Sony, Intel, Microsoft, IBM, Intel, Panasonic, Phillips, Pioneer, Motorola, Kenwood, Samsung, Toshiba, Dell, HP, Nokia, Macrovision e JVC. Possiamo trovare l'elenco completo su www.dlna.com.

:: Magie con Ubuntu

Gli strumenti con il logo DLNA ci offrono quindi la possibilità di "trafficare" con dispositivi normalmente ostici e già con Windows e i programmi proposti dall'associazione possiamo integrarli nella nostra rete. Chi ama addentrarsi un po' di più nel codice, però, tende a preferire Linux, per la sua maggiore elasticità. La prima cosa da fare, quindi, se vogliamo dedicarci ai dispositivi DNLA, è scaricare e installare una versione recente di Linux, se non l'abbiamo già. Il nostro consiglio è di orientarsi su Ubuntu: la sua versione 8.4 unisce la versatilità e la filosofia di condivisione caratteristiche di questo sistema operativo "libero" a una facilità d'uso veramente notevole. Troviamo tutto il necessario per installarla su www.

ubuntu-it.org. Una volta a posto con Linux, ci attrezzeremo con qualche strumento in più per fare la prima prova di lavoro in DNLA: trasformare il nostro computer in modo da condividere musica, foto e video e riprodurli sulla PlayStation3.

:: Scopriamo Fuppes

Per la nostra prova di lavoro abbiamo scelto di usare Fuppes. Si tratta di un media server gratuito multipiattaforma che offre numerose caratteristiche interessanti. Oltre a essere compatibile con i dispositivi DNLA e a funzionare su Linux, Windows, MacOS X e altri sistemi operativi Unix, integra la possibilità di convertire diversi formati di file, tra cui ogg, mpc, flac, aac/mp4, mp3, mp2, pcm e wav, è relativamente facile da configurare e ha una buona community di supporto e un forum che può sempre darci una mano (a condizione che sappiamo farci capire in inglese). Possiamo scaricare quel che ci serve dal sito http://fuppes.ulrich-voelkel.de/. Da qui possiamo accedere anche a un comodo wiki costantemente aggiornato.

:: Configuriamo il nostro sistema

Dopo aver installato Fuppes, seguiamo la procedura riportata qui sotto per configurare il nostro sistema. Prima di tutto modifichiamo il file di configurazione /etc/fuppes/fuppes.cfg e l'opzione dell'interfaccia. Nel nostro esempio useremo l'indirizzo IP 192.168.1.1.
<interface>192.168.1.1</interface>
Avviamo Fuppes e puntiamo il nostro sistema di navigazione per Internet all'indirizzo http://192.168.1.1:56596
/etc/init.d/fuppes restart
Selezioniamo l'opzione di configurazione nel menu sulla sinistra
Alla voce "ContentDirectory settings" -> Add objects, scriviamo il nome della directory in cui saranno contenuti i file da condividere e clicchiamo su "submit query"
Aggiungiamo tutte le cartelle che ci servono. Possiamo condividere anche un database iTunes.
Ricostruiamo il database multimediale. Per farlo selezioniamo Options nel menu sulla sinistra e clicchiamo su "rebuild database"

Possiamo verificare l'avanzamento del processo nella finestra di stato: man mano che i nostri contenuti sono indicizzati vediamo salire i contatori. Configuriamo il nostro computer in modo che possa essere riconosciuto dai client come server multimediale e creiamo un file /etc/network/if-up/fuppes come quello che segue (sostituendo l'interfaccia con quella che usiamo sul nostro computer)

```
#!/bin/bash
#
#  eth1 indica l'interfaccia WLAN usata nel test e andrà cambiata in base alla nostra configurazione
if [ "$IFACE" = "eth1" ]; then
        ip ro add 239.0.0.0/8 dev eth1
        /etc/init.d/fuppes restart &>/dev/null
fi
```

:: Iniziamo a divertirci

Per vedere che tutto abbia funzionato per il meglio colleghiamo e accendiamo la nostra PlayStation3, poi andiamo nella sezione Video e avviamo la ricerca dei media server. Dovremmo trovarne uno che si chiama fuppes. Dopo averlo selezionato entriamo in una cartella che contiene dei video e avviamone uno. Buon divertimento!

Nel blog bigg-theguilty.blogspot.com troverete postati alcuni esempi di compilazione per la vostra PS Linux MEdia Server.

PRIMI PASSI CON FUPPES

Dopo aver scaricato i sorgenti dal sito, scompattiamoli e installiamo il programma. Quando possiamo eseguire il programma correttamente digitando fuppes nella linea di comando, avviamolo una volta e poi usciamo. In questo modo creeremo il nostro file config in $HOME/.fuppes/fuppes.cfg. Potremo quindi modificarlo (possiamo trovare degli ottimi trucchi e consigli all'indirizzo http://fuppes.ulrich-voelkel.de/wiki/index.php?title=Basic_configuration). Iniziamo con delle operazioni semplici, come aggiungere un paio di directory di musica o foto. Specifichiamo una porta per l'interfaccia web (per esempio possiamo sostituire <http_port/> con <http_port>5080</http_port>) e ricordiamoci di usare una porta superiore a 1024. Se usiamo la PS3 o un qualsiasi altro dispositivo che ha una sezione specifica nel file di configurazione, dobbiamo impostare il suo attributo come "true". Per esempio <device name="PS3" enabled="false"> deve diventare <device name="PS3" enabled="true"> con la PlayStation3. A questo punto riavviamo fuppes nella root della console. Premiamo r per farci creare un database. Analizzerà le directory specificate nel file config. Comparirà un messaggio alla fine della procedura.

La MELA a rischio

Per anni si sono sentiti al sicuro ma con l'aumentare dei pc con sistema Mac Os X anche le minacce sono aumentate ed oggi gli utenti della mela devono iniziare a fare attenzione

I Mac: belli, eleganti, raffinati, ideali per grafici e musicisti e... immuni dagli attacchi dei pirati. Almeno, questo è quanto hanno sempre pensato gli utenti dei computer di Apple. In effetti, nel corso degli ultimi anni gli attacchi informatici ai sistemi Windows sono stati molto più diffusi di quelli nel mondo Macintosh ma questo non significa che le macchine di Apple siano meglio protette o i loro utenti più prudenti. Al contrario, la baldanza e la diffusa idea di essere invulnerabili a virus e malware in genere espone facilmente alle infezioni gli utenti Mac meno esperti, perché spesso non usano sistemi di protezione e controllo.

:: Un po' di storia

La presenza di malware per Macintosh non è storia recente. Anzi, il primo virus a diffondersi nelle case è stato prodotto proprio per questa piattaforma quando, nel 1982, Richard Skrenta scrisse il programma Elk Cloner che si diffondeva via floppy disk attaccandosi al sistema operativo di Apple. Anche prima dell'avvento dell'attuale Mac OS X, che è arrivato nel 2001 a sostituire il glorioso Mac Classic nato nel 1984, ci sono stati numerosi virus per Mac tra cui, nel 1987, nVir il cui codice fu diffuso dagli autori causando una marea di malware derivato. Apple ha introdotto in seguito delle

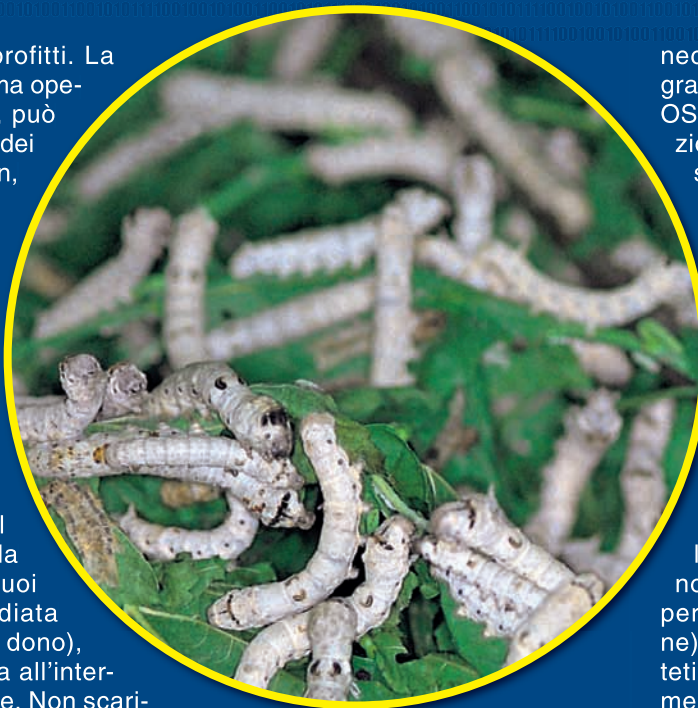
modifiche (come escludere la funzione di autorun che esegue automaticamente i programmi presenti su un disco quando questo viene inserito nel computer) e sono stati realizzati vari prodotti per la difesa dei suoi sistemi operativi ma per chi non usa protezioni i pericoli di infezione sono ancora presenti.

:: Il malware organizzato

Il rischio per gli utenti Macintosh è sempre maggiore con l'affermarsi di due fattori: la diffusione dei computer di Apple e l'organizzazione sistematica del mondo della pirateria informatica. Il fatto che i più recenti Mac siano oggetti di culto molto diffusi anche nell'ambiente del business rendono i suoi utenti molto più appetibili ai pirati, che oggi spesso non sono geni informatici in cerca di un modo alternativo per affermare la propria superiorità intellettuale ma vere e proprie organizzazioni criminali che

hanno in mente solo i profitti. La struttura stessa del sistema operativo Mac Os X, inoltre, può essere sfruttata da alcuni dei malware più diffusi: trojan, virus e worm.

:: Trojan, virus e worm

Per prima cosa cerchiamo di stabilire esattamente cosa distingue questi tre tipi di malware. Un Trojan (che prende il nome dal Cavallo di Troia, usato da Ulisse per introdurre i suoi soldati nella città assediata nascosti all'interno di un dono), è un malware che si cela all'interno di un'applicazione utile. Non scarichiamo un programmino che ci serve e, quando lo avviamo, a nostra insaputa lanciamo anche il software nocivo. I virus informatici, come quelli biologici, sono agenti infettivi che non possono riprodursi o crescere in assenza di un ospite. Hanno quindi bisogno di un programma da infettare e generalmente vengono eseguiti insieme a lui. I loro obiettivi sono due: propagarsi ad altri programmi ed (in genere) eseguire un compito, detto payload, che può andare dal visualizzare un messaggio a cancellare i contenuti del nostro hard disk o rubare i nostri dati personali. Un worm (che in inglese significa verme) è analogo a un virus ma non ha bisogno di un programma ospite per diffondersi. Analogamente al suo equivalente biologico, striscia per la rete informatica cercando di lasciare la propria progenie ovunque possibile.

I Mac sono vulnerabili a tutti e tre questi tre tipi di malware. La difesa contro i Trojan è implicitamente difficile su qualsiasi sistema operativo. OS X 10.5 Leopard ha introdotto un meccanismo che ci costringe a valutare quello che stiamo installando, facendo apparire una richiesta di conferma ogni volta che cerchiamo di installare un programma scaricato da Internet. Se però decidiamo di procedere i rischi a cui siamo esposti sono esattamente gli stessi a cui è vulnerabile un PC. Per quanto riguarda i virus, la loro prima necessità è quella di trovare un programma ospite in cui copiarsi e il Mac OS X non prevedere particolari protezioni per le applicazioni presenti sul sistema. Al contrario, l'architettura a bundle che adotta rende più facile nascondersi per i virus. Lo stesso vale per i worm. Un pirata potrebbe accedere al nostro sistema attraverso un Trojan e sfruttare la tecnologia di virus e worm per attaccare la nostra intera rete informatica. Il Mac OS X, inoltre, ha una gestione aperta della rubrica indirizzi. Questo è comodo perché ci permette di condividere dati tra le varie applicazioni che li usano (messaggerie, e-mail, eventuali periferiche compatibili come l'iPhone) ma consentirebbe a questo ipotetico malware di diffondersi rapidamente spedendosi ai nostri contatti. Se pensiamo che comprare un computer con il logo della mela sia una garanzia di protezione totale contro ogni attacco informatico, quindi, rivediamo la nostra posizione. E valutiamo la possibilità di comprare un buon antivirus...

I BUNDLE APPLICAZIONE

Una caratteristica del Mac OS che potrebbe tornare utile a un pirata sono i bundle applicazione. Sono dei documenti con l'estensione .app che appaiono all'utente come se fossero un file singolo ma sono in realtà delle directory con più livelli di contenuti. Tipicamente c'è una directory Contents che ne ospita una chiamata MacOS (che contiene l'eseguibile) e una detta Resources, che ha al suo interno le risorse dell'applicazione e le interfacce utente in tutte le lingue disponibili, archiviate all'interno di sotto-directory. In genere ci sono anche le directory Plugins, Frameworks e Shared Frameworks. Data la presenza di più eseguibili all'interno di queste strutture non sarebbe difficile per un pirata nascondere efficacemente del malware.

ARCH LINUX

La distribuzione da costruire pezzo per pezzo

Scopriamo insieme questa interessante distribuzione Linux: installiamola e prendiamo confidenza con alcuni dei suoi strumenti principali

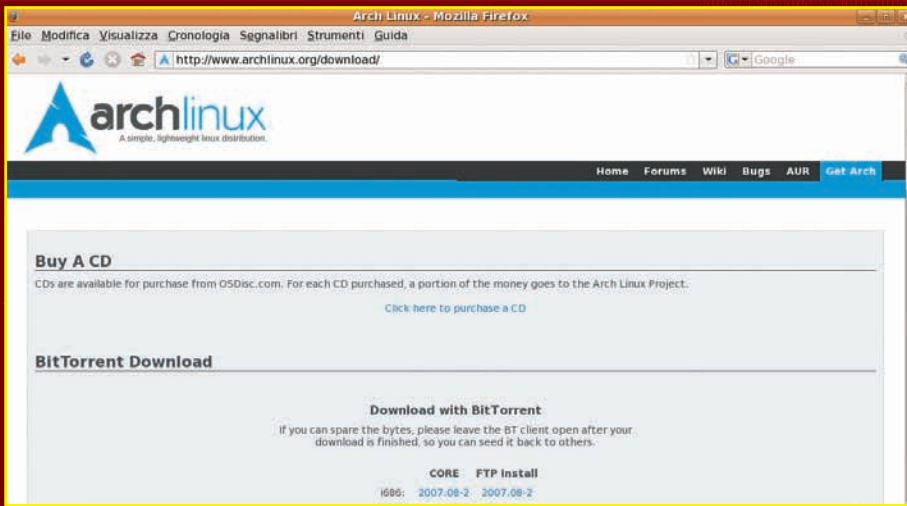
Le distribuzioni Linux per il desktop sono senz'altro quelle più visibili e note: Ubuntu, Fedora e Mandriva, solo per indicarne alcune delle principali. Esiste, però, una vasta schiera di distro che non mirano a conquistare l'utente alle prime armi ma che sono degne del massimo interesse, magari per alcune caratteristiche precipue o per prestazioni di tutto rispetto. Tra di esse spicca senz'altro Arch Linux.

:: Arch Linux, anatomia di una distribuzione

Si tratta di una distribuzione basata sul concetto di "rolling release": i pacchetti vengono costantemente aggiornati, mentre le release ufficiali non sono altro che delle mere "istantanee" che seguono i rilasci del kernel. Per questa ragione, una volta installato il sistema sul nostro PC non c'è alcun motivo per passare da una release ufficiale all'altra di Arch Linux: per avere il sistema sempre aggiornato è sufficiente aggiornare i singoli pacchetti che lo costituiscono.
Altra caratteristica di spicco di questa distro risiede nel ridotto numero di pacchetti installati per default; non c'è alcuna interfaccia grafica predefinita o, per meglio dire, non viene installata proprio alcuna interfaccia grafica: sta infatti all'utente scegliere quali software avere nel proprio sistema, pezzo per pezzo. Infine, tutti i pacchetti sono ottimizzati per le architetture i686 e x86-64; ciò, unito alla possibilità di installare solo i programmi strettamente necessari, rende questa distribuzione snella ed estremamente veloce.
Incuriositi? Andiamo allora ad installare Arch Linux.

:: La procedura di installazione

Apriamo con un web browser la pagina http://www.archlinux.org/download/ e scarichiamo tramite BitTorrent o HTTP/FTP l'immagine ISO dell'ultima versione di Arch Linux, Archlinux-i686-2007.08-2.core.iso. Poi masterizziamo il file ISO con un qualsiasi programma di masterizzazione come Nero (Windows) o K3b (Linux). Inseriamo il CD appena masterizzato e riavviamo il computer.

Nella schermata di avvio nella gran parte dei casi possiamo schiacciare semplicemente Invio per far effettuare il boot al sistema; in caso di problemi con l'hard disk digitiamo "arch ide-legacy" mentre se il PC si blocca duranta la procedura d'avvio scriviamo "arch noapic acpi=off pci=routeirq nosmp".

Da questa pagina scarichiamo l'ultima release ufficiale di Arch Linux.

```
Copyright 2002 - 2007 Judd Vinet <jvinet@zeroflux.org>
Distributed under the GNU General Public License (GPL)

ISOLINUX BOOT
Creation Tool: 'mkbootcd' written by Tobias Powalowski <tpowa@archlinux.org>

INSTALLATION SYSTEM
Arch Linux Don't Panic
Kernel: 2.6.22-ARCH
Architecture: i686
Creation Date: Wed Oct  3 13:40:13 UTC 2007

Available boot options (no input will boot the install/rescue system):
- 'arch <any_other_boot_option>' to boot the install/rescue system.
- 'arch root=/dev/??? <any_other_boot_option>' to boot into an existing system.
- 'lowmem <any_other_boot_option>' to boot the 96MB RAM install system.
- 'lowmem root=/dev/??? <any_other_boot_option>' to boot into an existing
  96MB RAM system.
- If you have trouble with IDE drives, use the "ide-legacy" boot option.
- If your system hangs during the boot process, any combinations of the
  boot options noapic acpi=off pci=routeirq nosmp may be useful.
- 'memtest' to start the memory test program memtest86+.

boot:
```

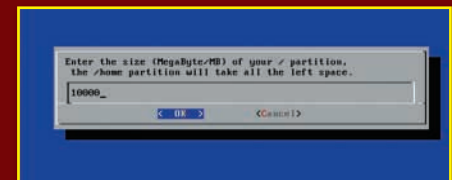
Ecco la schermata di avvio che compare dopo aver fatto il boot dal CD.

:: Avvio del sistema

A questo punto attendiamo che vengano caricati il kernel ed i servizi fondamentali. Schiacciamo poi Invio per far aprire una console di terminale. Quindi, lanciamo il comando "km" e nella schermata che appare selezioniamo tramite i tasti cursore il tipo di tastiera presente sul nostro PC (per una comune tastiera italiana il valore da selezionare è it.map.gz) e battiamo Invio. Premiamo il tasto Freccia Destra e schiacciamo nuovamente Invio per saltare il passaggio relativo alla scelta del font su schermo.
Siamo tornati al prompt della console. Adesso eseguiamo il comando "/arch/setup" per avviare il programma di installazione; questo utilizza un'interfaccia a caratteri che può apparire spartana ma che, in realtà, è davvero di facile uso. Per muoversi tra le opzioni si premono i tasti freccia, per spostarsi da un pulsante all'altro si schiaccia Tab mentre per confermare le scelte fatte si schiaccia Invio.
La prima schermata è di benvenuto. Premiamo Invio. Ora bisogna indicare la sorgente da usare per l'installazione: schiacciamo Invio per confermare "CD-ROM or OTHER SOURCE". Adesso comparirà il menu principale del programma di installazione: l'ordine delle varie voci segue l'ordine da seguire per portare a termine l'installazione.

Il programma di installazione di Arch Linux. Un po' spartano ma semplice da usare!

:: Le partizioni sull'hard disk

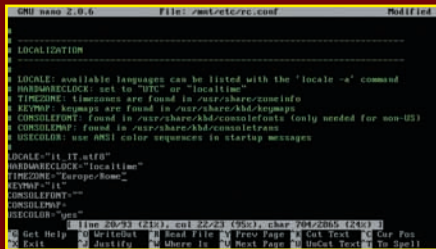
Selezioniamo la voce "Prepare Hard Drive". La prima operazione da compiere è partizionare il disco rigido. In questo articolo si presuppone che l'utente voglia dare ad Arch Linux l'intero spazio disponibile sull'hard disk: se si desidera un sistema dual boot con Windows si consulti la pagina all'indirizzo http://wiki.archlinux.org/index.php/Windows_and_Arch_Dual_Boot.
Nella schermata successiva lasciamo che il programma di installazione gestisca automaticamente il partizionamento del disco: selezioniamo l'opzione "Auto-Prepare". Quindi indichiamo le dimensioni della partizione /boot (quella contenente i file del kernel): 32 MB, il valore di default, sono più che sufficienti perciò schiacciamo semplicemente Invio. Anche le dimensioni predefinite della partizione di swap possono andar bene ma, per sicurezza, aumentiamo il valore fino a 512 MB. Poi stabiliamo le dimensioni della partizione root (/): alla partizione /home verrà riservato lo spazio rimanente sull'hard disk, quindi non diamo uno spazio eccessivo alla root altrimenti la partizione con i dati degli utenti risulterà troppo piccola. Nella schermata successiva indichiamo il filesystem da usare per / ed /home: ext3 è una buona scelta.

Una manciata di GB per la partizione root sono più che sufficienti...

:: Scegliere i pacchetti

Terminata la formattazione delle partizioni, si ritorna al menu principale. Selezioniamo la voce "Select Packages". Nella schermata successiva confermiamo con Invio l'opzione "Mount the CD-ROM". Battiamo Invio finché non ritorniamo al menu principale: abbiamo così selezionato i soli pacchetti di base.
Siamo arrivati al passaggio 3 dell'installazione. Evidenziamo la terza voce del menu "Install Packages" e schiacciamo Invio. Accettiamo le scelte di default per le successive schermate ed attendiamo che vengano installati sull'hard disk tutti i pacchetti.

I pacchetti principali vengono installati sull'hard disk.

:: Configurare il sistema

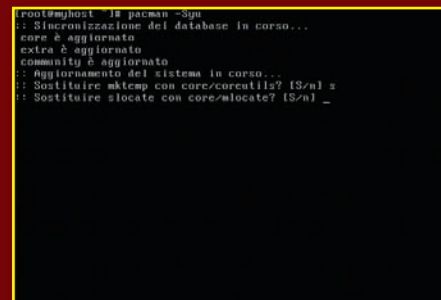
Dal menu principale selezioniamo "Configure System". Schiacciamo più volte Invio (le scelte di default dovrebbero andar bene nella gran parte dei casi) finché non appare la scritta "Select a Text Editor to Use". Qui scegliamo nano come editor. Nella schermata successiva, Configuration, compare un elenco dei file di configurazione che è possibile modificare: cominciamo con /etc/rc.conf, che in Arch Linux è il principale file di configurazione di sistema.
In questo file cambiamo la riga 'LOCALE="en_US.utf8"' in LOCALE="it_IT.utf8"' e la linea 'TIMEZONE="Canada/Pacific"' in 'TIMEZONE="Europe/Rome"'. Più in basso in /etc/rc.conf troviamo una riga che inizia con 'eth0=': questa è la linea contenente i parametri per la configurazione della rete; se per ottenere l'IP per l'interfaccia di rete sfruttiamo un server DHCP (è il caso tipico se si utilizza un router ADSL per la connessione ad Internet) cambiamo questa riga così: 'eth0="dhcp"'. Ora schiacciamo Ctrl + O ed Invio per salvare il file e Ctrl + X per uscire dall'editor.
Tornati nella schermata Configuration selezioniamo la voce Root-Password, quindi inseriamo la password per il superutente ed inseriamola poi nuovamente per conferma. Infine selezioniamo Pacman-Mirror e nella schermata che appare indichiamo come server principale ftp://mi.mirror.garr.it: in questo modo i pacchetti da scaricare verranno prelevati da un server vicino, aumentando così la velocità di download.

Modifichiamo /etc/rc.conf, il principale file di configurazione di sistema.

:: I ritocchi finali

Selezioniamo "Return to Main Menu". Nella schermata del menu principale scegliamo "Install Bootloader" ed accettiamo quindi il bootloader di default, GRUB. A questo punto verrà aperto il file di configurazione di GRUB: il file dovrebbe andar bene così come è, quindi usciamo semplicemente dall'editor con Ctrl + X. Installiamo il bootloader nel Master boot record schiacciando Invio. Per finire selezioniamo "Exit Install" e riavviamo il PC lanciando il comando "reboot".

:: Il primo avvio

Ora che il sistema è stato riavviato ci troviamo di fronte ad un nudo e crudo prompt nella console. Non rimane, quindi, che rimpolpare degnamente il parco software installato, costruendo da zero un sistema perfettamente tarato per i nostri bisogni.

Il programma da usare per gestire i pacchetti su Arch Linux si chiama pacman ed il suo utilizzo è molto semplice. Il primo comando da impartire dopo l'installazione iniziale è "pacman -Syu" che aggiorna i pacchetti presenti nel sistema, scaricando da Internet ogni aggiornamento disponibile. Fatto questo, avremo le ultimissime versioni dei programmi di base e saremo pronti per installare tutti i pacchetti che reputeremo necessari.

Per aggiornare tutti i pacchetti nel sistema basta lanciare "pacman -Syu".

:: La gestione dei pacchetti

Per installare un nuovo pacchetto lanciamo "pacman -S pacchetto". Ad esempio, per installare il file manager midnight commander (mc) digitiamo "pacman -S mc"; insieme al pacchetto verranno installate anche tutte le dipendenze richieste (ad esempio, le librerie che consentono il funzionamento di un programma).

Le ricerche tra i pacchetti si effettuano con il comando "pacman -Ss": ad esempio, per avere in console l'elenco dei pacchetti nei cui nomi è presente la stringa 'firefox' lanciamo "pacman -Ss firefox". Per eliminare un pacchetto e tutti i file che lo compongono, quindi, si usa il comando "pacman -R pacchetto".

In Arch Linux sono disponibili anche i cosiddetti "metapacchetti", cioè dei pacchetti fittizi che consentono di installare con facilità gruppi estesi di pacchetti. Un metapacchetto è ad esempio "gnome": installando questo è possibile avere nel proprio sistema tutti i pacchetti principali dell'ambiente grafico Gnome.

```
[root@myhost ~]# pacman -S gnome
:: gruppo gnome (include i pacchetti ignorati):
    epiphany  gnome-applets  gnome-backgrounds  gnome-control-center
    gnome-desktop  gnome-icon-theme  gnome-media  gnome-mime-data  gnome-mount
    gnome-panel  gnome-screensaver  gnome-session  gnome-settings-daemon
    gnome-themes  gnome-volume-manager  gnome2-user-docs  libgail-gnome
    metacity  nautilus  yelp
:: Installare l'intero contenuto? [S/n] _
```

Grazie a pacman ed ai metapacchetti possiamo installare un gruppo di pacchetti eseguendo un unico comando.

LAVORO, LAVORO, LAVORO...

:: Demoni e servizi

Con molte delle più diffuse distribuzioni la gestione dei servizi e dei demoni avviati al boot è del tutto automatizzata: si installa il pacchetto di un servizio ed il sistema provvede a lanciare ad ogni avvio lo script che lo attiva. Arch Linux, invece, lascia piena libertà all'utente e l'amministrazione dei servizi non fa eccezione.

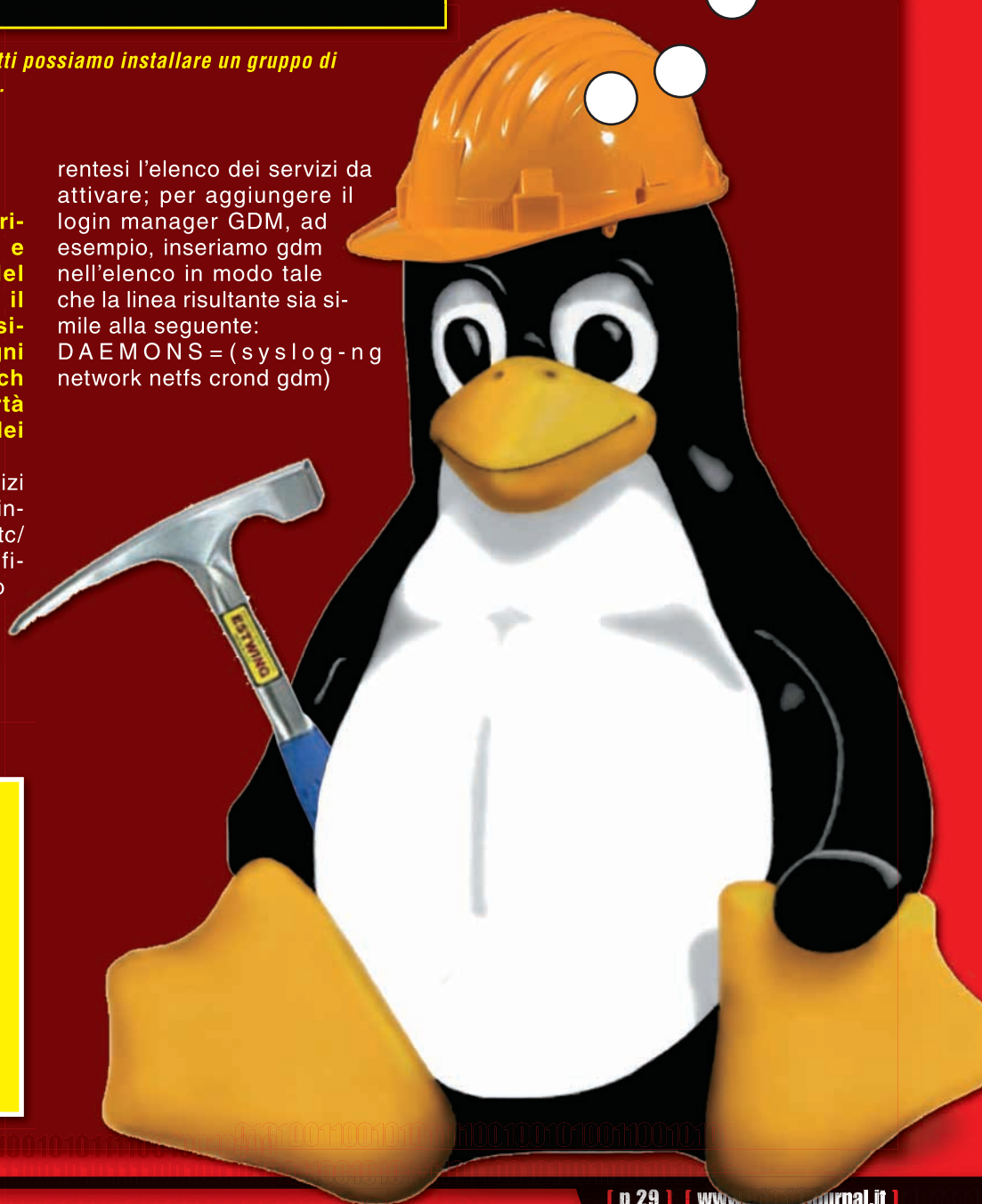
Per indicare al sistema quali servizi vogliamo attivare al boot si deve intervenire su di una riga del file /etc/rc.conf. Si apre con un editor il file (ad esempio tramite il comando "nano /etc/rc.conf") e si raggiunge la linea che inizia con DAEMONS. Questa contiene tra parentesi l'elenco dei servizi da attivare; per aggiungere il login manager GDM, ad esempio, inseriamo gdm nell'elenco in modo tale che la linea risultante sia simile alla seguente:

DAEMONS=(syslog-ng network netfs crond gdm)

LINK UTILI

www.archlinux.org/
Home page Arch Linux

http://wiki.archlinux.org/index.php/Official_Arch_Linux_Install_Guide
Guida all'installazione

http://wiki.archlinux.org/index.php/Beginners_Guide_(Italiano)
Guida per i nuovi utenti

WORM

I worm sono fra i programmi nocivi più diffusi e sono quelli il cui scopo è di replicarsi più velocemente possibile e colpire il maggior numero di computer. Conosciamoli meglio...

Un worm è un programma auto-replicante. Usa una rete per inviare copie di sé stesso ad altri sistemi e può farlo anche senza alcun intervento da parte dell'utente. Diversamente dal virus, non ha bisogno di collegarsi a un programma esistente. I worm danneggiano sempre la rete (se non altro consumando banda) e la usano come sistema di spostamento, mentre i virus infettano o danneggiano i file presenti sul computer colpito. Possono colpire anche la rete locale ma la presenza della rete non è essenziale per il loro funzionamento. Il primo virus worm fu creato da due ricercatori di Xerox PARC nel 1978. In origine, i ricercatori Shoch e Hupp crearono un worm in grado di individuare i processori inattivi sulla rete e di assegnare loro dei compiti, condividendo il carico di elaborazione e migliorando così l'efficienza dei processori di tutti i computer di una rete. Questi worm contenevano però delle limitazioni che impedivano loro di diffondersi più del dovuto. Da quel momento ne è passata di acqua sotto i ponti: oggi i worm sono fatti per diffondersi nel modo più ampio possibile e invece di aiutare i sistemi cercano di bloccarli.

PERCHÉ SI CHIAMANO WORM?

Il nome "worm" (verme) trae origine da The Shockwave Rider, un romanzo di fantascienza pubblicato nel 1975 da John Brunner. I ricercatori John F. Shoch e John A. Hupp di Xerox PARC scelsero di usare questo termine in un documento pubblicato nel 1982 (The Worm Programs, Comm ACM, 25(3):172-180, 1982) e da allora è entrato nell'uso comune.

:: Tipi di worm

I worm più famosi sono quelli che si diffondono tramite messaggi di posta elettronica. Tipicamente, il worm arriva con un messaggio di posta elettronica che nasconde il codice maligno nel corpo del messaggio o nell'allegato. In realtà, il codice può anche essere legato a un collegamento a un sito Web esterno. Nella maggior parte dei programmi di posta elettronica per attivare un worm bisogna aprire un allegato, facendo un bel doppio clic sulla sua icona o usando una opzione inclusa nel programma. D'altro canto, alcune versioni di altri programmi permettono al worm di attivarsi anche solo mostrando l'anteprima automatica del messaggio... Spesso un po' di furbizia (come per esempio l'oggetto del messaggio che contiene informazioni allettanti) è inoltre sufficiente a indurre l'utente a farlo, come dimostrano gli autori dei worm che sfruttano allegati con nomi esotici come "Immagini pornografiche gratuite" o altrettanto allettanti... Una volta attivato, il worm si diffonde usando sistemi di posta elettronica locali (come i servizi MS Outlook, la funzione MAPI di Windows) o direttamente tramite SMTP, usando cioè un sistema interno al worm per spedire i messaggi. Gli indirizzi che invia vengono spesso prelevati dal programma di e-mail o dai file dei computer infettati. A partire da Klez.E del 2002, i worm che usano l'SMTP camuffano l'indirizzo del mittente, in modo che i destinatari delle e-mail infettate non capiscano che i messaggi provengono dall'indirizzo riportato nel campo "Da" del messaggio stesso (indirizzo del mittente). I worm delle messaggerie si propagano invece tramite applicazioni di messaggeria istantanea, attraverso l'invio di collegamenti a siti infetti a tutti i contatti presenti nella rubrica locale. L'unica differenza tra questi worm e quelli via e-mail è il metodo usato per inviare i collegamenti. MSN, ICQ e programmi simili sono tutti potenziali veicoli di diffusione. Il bersaglio principale invece dei worm IRC sono i canali di chat. Viene usato lo stesso metodo di

infezione e di diffusione dei due worm precedenti, ossia l'invio di file infetti o collegamenti a siti infetti. L'invio di file infetti è meno efficace, in quanto il destinatario deve confermare la ricezione, salvare il file e aprirlo perché l'infezione abbia luogo. Neanche i programmi di condivisione file sono immuni dai worm. Il codice maligno in questione crea una copia di sé stesso in una cartella condivisa, per lo più situata sul sistema locale e si dà un nome interessante. A quel punto è pronto per essere scaricato tramite rete P2P e propagare così la diffusione del file infetto. I worm possono scegliere di usare un nome semplicemente curioso oppure un nome di un file molto diffuso, come un film o una canzone. I worm del Web invece sono quelli che prendono di mira direttamente le porte TCP/IP meno trafficate, invece di usare i protocolli molto diffusi come la posta elettronica o IRC. Un esempio classico è "Blaster", che sfruttava un punto debole di Windows. Il sistema infetto esamina computer scelti a caso sia sulla rete locale sia su Internet, cercando di attaccare la porta 135. Se ci riesce, il worm viene inoculato nel computer di nascosto.

:: Cos'è un payload?

Un "payload" è letteralmente il carico che viene consegnato. Tecnicamente è quello che i worm depositano sul computer. Più praticamente, è un programma che non si limita a diffondere il worm: può eliminare file sul sistema ospite, criptare documenti per poi permettere ai pirati di chiederci un riscatto per ottenerne nuovamente il controllo o inviare documenti via posta elettronica. Un classico payload per i worm consiste nell'installazione di una backdoor (un accesso nascosto, di cui parliamo nella sezione relativa) sul computer infetto, che mette il nostro PC sotto il controllo dal creatore del worm. Sobig e Mydoom sono esempi di worm creatori di zombie. Le reti di computer di questo tipo sono spesso definite "botnet" e sono molto usate dai propagatori di spam per l'invio di messaggi indesiderati o per camuffare l'indirizzo del loro sito. Alla fine quindi spesso sono gli autori di messaggi spam a finanziare la creazione di questi worm e alcuni creatori sono stati colti nell'atto di vendere elenchi di indirizzi di computer infetti.

:: Il primo virus worm dell'era moderna

Il worm Melissa, noto anche come "Mailissa", "Simpsons", "Kwyjibo" o "Kwejeebo", è un virus macro che arriva per posta elettronica, il che ha indotto alcuni a classificarlo come worm. Individuato per la prima volta il 26 marzo 1999, Melissa bloccava i sistemi di posta elettronica, intasandoli di e-mail infette propagate dal worm. Melissa è stato diffuso per la prima volta nel gruppo di discussione Usenet alt.sex. Il virus era nascosto in un file denominato "List.DOC" che conteneva password che consentivano l'accesso a 80 siti Web pornografici.

La versione originale del worm è stata inviata via e-mail a tantissime persone. Melissa era opera dell'americano David L. Smith e prendeva nome da una ballerina di lap dance da lui conosciuta in Florida. Il creatore del virus si faceva chiamare Kwyjibo ma fu identificato come l'autore di virus macro che si nascondeva dietro gli pseudonimi VicodinES e Alt-F11.

L'autore è stato identificato semplicemente perché usava numerosi file di Microsoft Word che presentavano lo stesso Globally Unique Identifier (GUID), un numero di serie generato precedentemente sulla base dell'indirizzo della scheda di rete presente in ogni computer. Smith fu condannato a 10 anni ma scontò in definitiva solo 20 mesi in un carcere federale americano e dovette pagare una multa di 5.000 dollari.

Melissa può diffondersi tramite i programmi di elaborazione di testi Microsoft Word 97 e Word 2000. Può propagarsi in massa via posta elettronica usando i progammi per e-mail Microsoft Outlook 97 o Outlook 98.

Il worm non funziona su altre versioni di Word come Word 95 e non può propagarsi via posta elettronica usando altri programmi, compreso Outlook Express.
Se un documento di Word che contiene il virus (che si tratti di LIST.DOC o di un altro file che è stato successivamente infettato) viene scaricato e aperto, la macro contenuta nel documento entra in funzione e cerca di propagare il worm via posta elettronica.

Quando la macro inizia l'invio di massa di e-mail, rileva i primi 50 contatti della rubrica dell'utente e invia i messaggi ai corrispondenti indirizzi. Ecco come si presenta un messaggio infetto:

```
Da: <nome del mittente infetto>

Oggetto: Important message from
<nome del mittente>

A: <Destinatari, tratti dai 50
contatti>

Allegato: LIST.DOC
```

Corpo del messaggio: Here is that document you asked for ... don't show anyone else ;-)

Se il worm è già stato inviato o non può diffondersi con questo sistema per assenza di una connessione a Internet o di Outlook, contagia altri documenti di Word presenti sul computer. Anche se gli altri documenti infetti non possono essere spediti subito via e-mail possono ovviamente passare di mano in mano, o di CD-ROM in CD-ROM, e diffondere l'infezione. Tra l'altro, se il documento contiene dati riservati, il destinatario del messaggio che contiene il documento può visualizzarli. Si tratta quindi di un sistema di infezione praticamente a prova di bomba e dalle potenzialità assolutamente devastanti.
La routine di attivazione del worm inserisce citazioni tratte dal programma di animazione televisivo I Simpsons in altri documenti quando la cifra dei minuti dell'ora indicata dall'orologio interno del computer corrisponde a quella del giorno del mese (per esempio, alle 7:09 del giorno 9).

Un esempio di citazione è "Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here" ("Ventidue punti, più triplo punteggio parola, più cinquanta punti per aver usato tutte le mie lettere. Fine del gioco. Me ne vado", un riferimento al gioco dello Scarabeo).